IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor:	: **Masaaki TAKASE**
Filed	: **Concurrently herewith**
For	: **KEY EXCHANGE PROXY....**
Serial No.	: **Concurrently herewith**

September 30, 2003

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

PRIORITY CLAIM AND

SUBMISSION OF PRIORITY DOCUMENT

S I R:

Applicant hereby claims priority under 35 USC 119 from **Japanese** patent application number **2002-288476** filed **October 1, 2002,** a copy of which is enclosed.

Respectfully submitted,

Thomas J. Bean
Reg. No. 44,528

Katten Muchin Zavis Rosenman
575 Madison Avenue
New York, NY 10022-2585
(212) 940-8800
Docket No.: FUJH 20.637

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００２年１０月　１日

出願番号
Application Number: 特願２００２－２８８４７６

[ST. 10/C]: [ＪＰ２００２－２８８４７６]

出願人
Applicant(s): 富士通株式会社

２００３年　８月　１日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００３－３０６１９０５

【書類名】　特許願
【整理番号】　0251633
【提出日】　平成14年10月 1日
【あて先】　特許庁長官　殿
【国際特許分類】　H04L　9/08
　　G09C　1/00
【発明の名称】　鍵交換代理ネットワークシステム
【請求項の数】　10
【発明者】
　【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
　【氏名】　高瀬　正明
【特許出願人】
　【識別番号】　000005223
　【氏名又は名称】　富士通株式会社
【代理人】
　【識別番号】　100094514
　【弁理士】
　【氏名又は名称】　林　恒徳
【選任した代理人】
　【識別番号】　100094525
　【弁理士】
　【氏名又は名称】　土井　健二
【手数料の表示】
　【予納台帳番号】　030708
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9704944

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　鍵交換代理ネットワークシステム

【特許請求の範囲】

【請求項１】　暗号通信を行う第１および第２の端末装置の間で行われる鍵交換処理を代行する鍵交換代理ネットワークシステムであって，

前記第１の端末装置にアクセスされる第１のサービス制御装置および前記第１の端末装置の鍵交換処理を代行する第１の鍵交換代理装置を備え，

前記第１のサービス制御装置は，

前記第１もしくは第２の端末装置または前記第１の鍵交換代理装置からのメッセージを受信する第１のメッセージ受信部と，

前記第１のメッセージ受信部により受信されたメッセージが鍵交換メッセージまたは鍵を含むメッセージかどうかを判断するための第１のデータを保持し，該第１のデータに基づいて前記受信メッセージが前記鍵交換メッセージまたは前記鍵を含むメッセージかどうかを判断し，前記受信メッセージが前記第１または第２の端末装置からの鍵交換メッセージの場合には転送先を前記第１の鍵交換代理装置とし，前記受信メッセージが前記第１の鍵交換代理装置からの鍵交換メッセージの場合には転送先を前記第２の端末装置とし，前記受信メッセージが前記鍵を含むメッセージの場合には転送先を前記第１の端末装置として決定する第１のプロトコル制御部と，

前記第１のプロトコル制御部により決定された転送先に前記第１のメッセージ受信部により受信されたメッセージを送信する第１のメッセージ送信部と，

を備え，

前記第１の鍵交換代理装置は，

前記第１のサービス制御装置からのメッセージを受信する第２のメッセージ受信部と，

前記第２のメッセージ受信部により受信されたメッセージが前記鍵交換メッセージである場合に，前記第２の端末装置との間で前記鍵交換メッセージを交換して鍵を決定する第２のプロトコル制御部と，

前記第２のプロトコル制御部により決定された前記鍵を，前記鍵を含むメッセ

ージとして前記第１のサービス制御装置宛てに送信する第２のメッセージ送信部と，

を備えている鍵交換代理ネットワークシステム。

【請求項２】　請求項１において，

前記第２のプロトコル制御部は，前記第１の端末装置からの鍵交換メッセージの受信を契機として前記第２の端末装置との間で鍵を決定する，鍵交換ネットワークシステム。

【請求項３】　請求項１において，

前記第２のプロトコル制御部は，前記第２の端末装置からの鍵交換メッセージの受信を契機として前記第２の端末装置との間で鍵を決定する，鍵交換ネットワークシステム。

【請求項４】　請求項１から３のいずれか１項において，

前記第２の端末装置にアクセスされる第２のサービス制御装置および前記第２の端末装置の鍵交換処理を代行する第２の鍵交換代理装置をさらに備え，

前記第２のサービス制御装置は，

前記第１もしくは第２の端末装置または前記第２の鍵交換代理装置からのメッセージを受信する第３のメッセージ受信部と，

前記第３のメッセージ受信部により受信されたメッセージが鍵交換メッセージまたは鍵を含むメッセージかどうかを判断するための第２のデータを保持し，該第２のデータに基づいて前記受信メッセージが前記鍵交換メッセージまたは前記鍵を含むメッセージかどうかを判断し，前記受信メッセージが前記第１または第２の端末装置からの鍵交換メッセージの場合には転送先を前記第２の鍵交換代理装置とし，前記受信メッセージが前記第２の鍵交換代理装置からの鍵交換メッセージの場合には転送先を前記第１の端末装置とし，前記受信メッセージが前記鍵を含むメッセージの場合には転送先を前記第２の端末装置として決定する第３のプロトコル制御部と，

前記第３のプロトコル制御部により決定された転送先に前記第３のメッセージ受信部により受信されたメッセージを送信する第３のメッセージ送信部と，

を備え，

前記第２の鍵交換代理装置は，

前記第２のサービス制御装置からのメッセージを受信する第４のメッセージ受信部と，

前記第４のメッセージ受信部により受信されたメッセージが前記鍵交換メッセージである場合に，前記第１の鍵交換代理装置との間で前記鍵交換メッセージを交換して鍵を決定する第４のプロトコル制御部と，

前記第４のプロトコル制御部により決定された前記鍵を，前記鍵を含むメッセージとして前記第２のサービス制御装置宛てに送信する第４のメッセージ送信部と，

を備えている鍵交換代理ネットワークシステム。

【請求項５】　請求項４において，

前記第１および第２のサービス制御装置が同一の装置により構成される，鍵交換代理ネットワークシステム。

【請求項６】　暗号通信を行う第１および第２の端末装置の間で行われる鍵交換処理を代行する鍵交換代理ネットワークシステムであって，

前記第１の端末装置にアクセスされるサービス制御装置および前記第１の端末装置の鍵交換処理を代行する鍵交換代理装置を備え，

前記サービス制御装置は，受信メッセージの転送先を判断するためのサービスプロファイルに基づいて，前記第１の端末装置からの鍵交換代理要求メッセージまたは前記第２の端末装置からの鍵交換メッセージを前記鍵交換代理装置に転送し，前記鍵交換代理装置からの鍵交換メッセージを前記第２の端末装置に転送するとともに，前記鍵交換代理装置からの鍵を含むメッセージを前記第１の端末装置に転送し，

前記鍵交換代理装置は，前記鍵交換メッセージを前記第２の端末装置との間で前記サービス制御装置を介して交換して鍵を決定し，決定した鍵を含むメッセージを前記サービス制御装置を介して前記第１の端末装置に送信する，

鍵交換代理ネットワークシステム。

【請求項７】　端末装置によりアクセスされ，該端末装置，該端末装置の鍵交換処理を代行する鍵交換代理装置，または該端末装置と暗号通信を行う通信相

手端末からのメッセージを転送するサービス制御装置であって，

前記端末装置，前記鍵交換代理装置，または前記通信相手端末装置からのメッセージを受信するメッセージ受信部と，

前記メッセージ受信部により受信されたメッセージが鍵交換メッセージまたは鍵を含むメッセージかどうかを判断するためのデータを保持し，該データに基づいて前記受信メッセージが前記鍵交換メッセージまたは前記鍵を含むメッセージかどうかを判断し，前記受信メッセージが前記端末装置または通信相手端末装置からの鍵交換メッセージの場合には転送先を前記鍵交換代理装置とし，前記受信メッセージが前記鍵交換代理装置からの鍵交換メッセージの場合には転送先を前記通信相手端末装置とし，前記受信メッセージが前記鍵を含むメッセージの場合には転送先を前記端末装置として決定するプロトコル制御部と，

前記プロトコル制御部により決定された転送先に前記受信メッセージを送信するメッセージ送信部と，

を備えているサービス制御装置。

【請求項８】　通信相手端末装置と暗号通信を行う端末装置に代わって前記通信相手端末との間で鍵交換処理を行う鍵交換代理装置であって，

前記端末装置にアクセスされ，前記端末装置または前記通信相手端末装置からのメッセージを転送するサービス制御装置からのメッセージを受信するメッセージ受信部と，

前記メッセージ受信部により受信されたメッセージが鍵交換メッセージである場合に，前記通信相手端末装置との間で前記鍵交換メッセージを交換して鍵を決定するプロトコル制御部と，

前記プロトコル制御部により決定された前記鍵を，前記鍵を含むメッセージとして前記サービス制御装置宛てに送信するメッセージ送信部と，

を備えている鍵交換代理装置。

【請求項９】　通信ネットワークのサービス制御装置にアクセスして，通信相手端末装置と暗号通信を行う端末装置であって，

暗号化が必要な通信の条件を規定した第１のデータおよび暗号化に使用される鍵を含む第２のデータを保持し，前記第１のデータに基づいて通信相手端末装置

との通信に暗号化が必要かどうかを判断し，暗号化に必要な鍵が前記第２のデータに存在するかどうかを判断する暗号処理管理部と，

前記暗号処理管理部により暗号化が必要であると判断され，かつ，暗号化に必要な鍵が存在しないと判断された場合に，鍵交換メッセージを前記サービス制御装置を介して前記通信相手端末宛てに送信するメッセージ送信部と，

前記通信ネットワークの鍵交換代理装置と前記通信相手端末装置との間で決定された鍵を含むメッセージを前記サービス制御装置から受信するメッセージ受信部と，

を備えている端末装置。

【請求項１０】　暗号通信を行う第１および第２の端末装置の間で行われる鍵交換処理を前記第１の端末装置に代わって行う鍵交換代理装置および前記第１の端末装置にアクセスされるサービス制御装置を有する鍵交換代理ネットワークシステムで実行される鍵交換代理方法であって，

前記サービス制御装置において，前記第１または第２の端末装置から送信される鍵交換メッセージを前記鍵交換代理装置に転送し，

前記鍵交換代理装置において，前記第１の端末装置と前記第２の端末装置との間で交換される鍵交換メッセージを作成して前記サービス制御装置に送信し，

前記サービス制御装置において，前記鍵交換メッセージを前記第２の端末装置に転送し，

前記鍵交換代理装置において，前記鍵交換メッセージの交換により決定された鍵を含むメッセージを前記サービス制御装置に送信し，

前記サービス制御装置において，前記鍵交換代理装置から送信された前記鍵を含むメッセージを前記第１の端末装置に転送する，

鍵交換代理方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は，通信端末間での暗号鍵の交換を代理する鍵交換代理ネットワークシステムに関し，特に，ＩＰＳｅｃにおいて必要となる鍵の交換を代理する鍵交換

代理ネットワークシステムに関する。

【０００２】

また，本発明は，鍵交換代理ネットワークシステムにおける端末装置，サービス制御装置，および鍵交換代理装置に関する。

【０００３】

【従来の技術】

インターネットの急速な発展によりＩＰパケットのトラヒックが急増している。また，携帯電話の普及に伴い，ＩＭＴ－２０００（International Mobile Telecommunications 2000）での標準化，実用化の動きもあり，モバイル環境での高速ＩＰ通信が普及すると考えられる。

【０００４】

モバイル環境でのＩＰ通信では，従来のＩＰｖ４ではアドレス枯渇の問題があるので，ＩＰｖ６が必須となっている。このＩＰｖ６環境では，サーバ等の端末にＩＰＳｅｃ／ＩＫＥ（IP Security / Internet Key Exchange）が必須となっているので，ＩＰＳｅｃを用いた安全な通信が提供されると考えられる。

【０００５】

しかし，ＩＰＳｅｃ／ＩＫＥでは，端末に鍵交換サーバ（ＩＫＥサーバ）を搭載する必要がある。この鍵交換サーバは複雑な処理を行うため，端末には，比較的高速な処理装置（ＣＰＵ等）と大きなメモリが必要となる。

【０００６】

したがって，パソコンやサーバ等の端末には，ＩＰＳｅｃ／ＩＫＥの導入が容易である一方，小型軽量化が要求される携帯電話やＰＤＡ（Personal Digital Assistant）等の携帯端末にＩＰＳｅｃ／ＩＫＥを導入するには，難点がある。

【０００７】

たとえば，一般的に安全でない通信路で安全に鍵交換を行う方法としてDiffie-Hellmanの鍵交換方法があるが，この方法を実行するには，鍵交換を行う端末においてべき乗計算を行う必要があるため，端末のリソースを消費し，携帯端末には大きな負荷となる。

【０００８】

また，ＩＰＳｅｃ／ＩＫＥの処理には電力を多く必要とするので，携帯端末における消費電力という観点からも，ＩＰＳｅｃ／ＩＫＥを携帯端末に搭載するのは現実的ではない。このため，携帯端末自身にはなるべく機能追加を行わずに，ＩＰＳｅｃ／ＩＫＥによるサービスを行うことが求められている。

【０００９】

そこで，鍵交換処理を携帯端末が行うのではなく，他の装置に代行させる技術が考えられ，このような技術として，ユーザ端末機器からアクセスされるホームサーバ等の装置が代行するものがある（たとえば，特許文献１参照）。

【００１０】

【特許文献１】

特開２００２－１５８６５０号公報（図１等）

【００１１】

【発明が解決しようとする課題】

しかし，この従来の技術によると，ユーザ端末機器がホームサーバ等の代行サーバに直接アクセスするので，ユーザ端末機器は代行サーバのアドレスを知っている必要がある。この場合に，ユーザ端末機器と通信を行う相手端末機器は，必ずしも代行サーバのアドレスを知っているとは限らないので，相手端末機器から通信を開始して鍵交換を行うことはできない。したがって，適用の範囲が，ユーザ端末機器から通信を開始する場合に限定される。

【００１２】

本発明は，このような背景に鑑みなされたものであり，その目的は，鍵交換に伴う処理をネットワーク側の装置に代行させて，端末の負荷を軽減することにある。

【００１３】

また，本発明の目的は，暗号通信を行う２つの端末のいずから鍵交換処理の要求があっても鍵交換処理の代行が可能な鍵交換方式を提供することにある。

【００１４】

【課題を解決するための手段】

前記目的を達成するために，本発明による鍵交換代理ネットワークシステムは

，暗号通信を行う第１および第２の端末装置の間で行われる鍵交換処理を代行する鍵交換代理ネットワークシステムであって，前記第１の端末装置にアクセスされる第１のサービス制御装置および前記第１の端末装置の鍵交換処理を代行する第１の鍵交換代理装置を備え，前記第１のサービス制御装置は，前記第１もしくは第２の端末装置または前記第１の鍵交換代理装置からのメッセージを受信する第１のメッセージ受信部と，前記第１のメッセージ受信部により受信されたメッセージが鍵交換メッセージまたは鍵を含むメッセージかどうかを判断するための第１のデータを保持し，該第１のデータに基づいて前記受信メッセージが前記鍵交換メッセージまたは前記鍵を含むメッセージかどうかを判断し，前記受信メッセージが前記第１または第２の端末装置からの鍵交換メッセージの場合には転送先を前記第１の鍵交換代理装置とし，前記受信メッセージが前記第１の鍵交換代理装置からの鍵交換メッセージの場合には転送先を前記第２の端末装置とし，前記受信メッセージが前記鍵を含むメッセージの場合には転送先を前記第１の端末装置として決定する第１のプロトコル制御部と，前記第１のプロトコル制御部により決定された転送先に前記第１のメッセージ受信部により受信されたメッセージを送信する第１のメッセージ送信部と，を備え，前記第１の鍵交換代理装置は，前記第１のサービス制御装置からのメッセージを受信する第２のメッセージ受信部と，前記第２のメッセージ受信部により受信されたメッセージが前記鍵交換メッセージである場合に，前記第２の端末装置との間で前記鍵交換メッセージを交換して鍵を決定する第２のプロトコル制御部と，前記第２のプロトコル制御部により決定された前記鍵を，前記鍵を含むメッセージとして前記第１のサービス制御装置宛てに送信する第２のメッセージ送信部と，を備えている。

【００１５】

本発明による鍵交換代理ネットワークシステムは，通信相手端末装置と暗号通信を行う端末装置に代わって前記通信相手端末との間で鍵交換処理を行う鍵交換代理装置であって，前記端末装置にアクセスされ，前記端末装置または前記通信相手端末装置からのメッセージを転送するサービス制御装置からのメッセージを受信するメッセージ受信部と，前記メッセージ受信部により受信されたメッセージが鍵交換メッセージである場合に，前記通信相手端末装置との間で前記鍵交換

メッセージを交換して鍵を決定するプロトコル制御部と，前記プロトコル制御部により決定された前記鍵を，前記鍵を含むメッセージとして前記サービス制御装置宛てに送信するメッセージ送信部と，を備えている。

【００１６】

本発明による鍵交換代理方法は，暗号通信を行う第１および第２の端末装置の間で行われる鍵交換処理を前記第１の端末装置に代わって行う鍵交換代理装置および前記第１の端末装置にアクセスされるサービス制御装置を有する鍵交換代理ネットワークシステムで実行される鍵交換代理方法であって，前記サービス制御装置において，前記第１または第２の端末装置から送信される鍵交換メッセージを前記鍵交換代理装置に転送し，前記鍵交換代理装置において，前記第１の端末装置と前記第２の端末装置との間で交換される鍵交換メッセージを作成して前記サービス制御装置に送信し，前記サービス制御装置において，前記鍵交換メッセージを前記第２の端末装置に転送し，前記鍵交換代理装置において，前記鍵交換メッセージの交換により決定された鍵を含むメッセージを前記サービス制御装置に送信し，前記サービス制御装置において，前記鍵交換代理装置から送信された前記鍵を含むメッセージを前記第１の端末装置に転送する，ものである。

【００１７】

本発明によると，第１または第２の端末装置からサービス制御装置に送信された鍵交換メッセージは，サービス制御装置によって鍵交換代理装置に転送される。その後，鍵交換代理装置と第２の端末装置との間で鍵交換処理が行われ，暗号通信に必要な鍵が決定される。決定された鍵は第１の端末装置に送信される。

【００１８】

したがって，本発明によると，第１の端末装置は，鍵交換および鍵決定に必要な処理を行うことなく，暗号通信に必要な鍵を得ることができる。その結果，第１の端末装置の負荷を軽減することができる。

【００１９】

また，サービス制御装置は，第１または第２の端末装置からの鍵交換メッセージを鍵交換代理装置に転送する。したがって，第１の端末装置は，第２の端末装置の宛先アドレスを知っているだけでよく，また，第２の端末装置は第１の端末

装置の宛先アドレスを知っているだけでよい。このため，第１および第２の端末装置のいずから鍵交換処理の要求があっても鍵交換処理の代行が可能である。

【００２０】

本発明によるサービス制御装置は，端末装置によりアクセスされ，該端末装置，該端末装置の鍵交換処理を代行する鍵交換代理装置，または該端末装置と暗号通信を行う通信相手端末からのメッセージを転送するサービス制御装置であって，前記端末装置，前記鍵交換代理装置，または前記通信相手端末装置からのメッセージを受信するメッセージ受信部と，前記メッセージ受信部により受信されたメッセージが鍵交換メッセージまたは鍵を含むメッセージかどうかを判断するためのデータを保持し，該データに基づいて前記受信メッセージが前記鍵交換メッセージまたは前記鍵を含むメッセージかどうかを判断し，前記受信メッセージが前記端末装置または通信相手端末装置からの鍵交換メッセージの場合には転送先を前記鍵交換代理装置とし，前記受信メッセージが前記鍵交換代理装置からの鍵交換メッセージの場合には転送先を前記通信相手端末装置とし，前記受信メッセージが前記鍵を含むメッセージの場合には転送先を前記端末装置として決定するプロトコル制御部と，前記プロトコル制御部により決定された転送先に前記受信メッセージを送信するメッセージ送信部と，を備えている。

【００２１】

本発明による鍵交換代理装置は，通信相手端末装置と暗号通信を行う端末装置に代わって前記通信相手端末との間で鍵交換処理を行う鍵交換代理装置であって，前記端末装置にアクセスされ，前記端末装置または前記通信相手端末装置からのメッセージを転送するサービス制御装置からのメッセージを受信するメッセージ受信部と，前記メッセージ受信部により受信されたメッセージが鍵交換メッセージである場合に，前記通信相手端末装置との間で前記鍵交換メッセージを交換して鍵を決定するプロトコル制御部と，前記プロトコル制御部により決定された前記鍵を，前記鍵を含むメッセージとして前記サービス制御装置宛てに送信するメッセージ送信部と，を備えている。

【００２２】

本発明による端末装置は，通信ネットワークのサービス制御装置にアクセスし

て，通信相手端末装置と暗号通信を行う端末装置であって，暗号化が必要な通信の条件を規定した第１のデータおよび暗号化に使用される鍵を含む第２のデータを保持し，前記第１のデータに基づいて通信相手端末装置との通信に暗号化が必要かどうかを判断し，暗号化に必要な鍵が前記第２のデータに存在するかどうかを判断する暗号処理管理部と，前記暗号処理管理部により暗号化が必要であると判断され，かつ，暗号化に必要な鍵が存在しないと判断された場合に，鍵交換メッセージを前記サービス制御装置を介して前記通信相手端末宛てに送信するメッセージ送信部と，前記通信ネットワークの鍵交換代理装置と前記通信相手端末装置との間で決定された鍵を含むメッセージを前記サービス制御装置から受信するメッセージ受信部と，を備えている。

【００２３】

【発明の実施の形態】

図１は，本発明の実施の形態による鍵交換代理ネットワークシステムの構成を示すブロック図である。この鍵交換代理ネットワークシステムは，サービス制御装置１，鍵交換代理サーバ２，認証サーバ３，ルータ４，加入者端末５，および通信相手端末６を有する。

【００２４】

サービス制御装置１，鍵交換代理サーバ２，認証サーバ３，およびルータ４は，コアネットワーク（たとえばインターネット）７に接続され，相互に通信可能になっている。

【００２５】

サービス制御装置１は，たとえばコアネットワーク７のエッジルータ（エッジノード）であり，モバイルＩＰやモバイルＩＰｖ６では，携帯端末（たとえば加入者端末５）と無線通信を行うノードである。

【００２６】

サービス制御装置１は，鍵交換代理サーバ２のＩＰアドレスをあらかじめ知っているとともに，加入者端末５が位置登録を行った際に認証サーバ３から与えられるサービスプロファイル（後述）を保持する。

【００２７】

このサービスプロファイルにより，サービス制御装置１は，鍵交換処理に伴い転送すべきパケットと通常のルーティングを行うパケットとを区別し，鍵交換処理に伴い転送すべきパケット（後述する鍵交換メッセージ，鍵を含むメッセージ等）を鍵交換代理サーバ２または加入者端末５に転送する。

【００２８】

加入者端末５は，たとえば携帯端末（携帯電話，ＰＤＡ等）であり，無線回線を介してサービス制御装置１に接続される。したがって，加入者端末５から送信されるパケットおよび加入端末５宛てに送信されるパケットはサービス制御装置１を経由するようになっている。また，加入者端末５は，本実施の形態では，装置の小型・軽量化や低消費電力化のため，鍵交換サーバ（ＩＫＥサーバ，鍵交換プログラム）を搭載していない。

【００２９】

通信相手端末６は，ルータ４に接続され，本実施の形態では，コアネットワーク７を介して加入者端末５と通信を行う端末である。この通信相手端末６は，たとえばコンピュータ，サーバ（たとえば電子商取引サーバ）等であり，鍵交換サーバ（ＩＫＥサーバ，鍵交換プログラム）を搭載している。

【００３０】

鍵交換代理サーバ２は，加入者端末５が鍵交換サーバを搭載していないことから，加入者端末５に代わり，ＩＰＳｅｃ／ＩＫＥ（IP Security / Internet Key Exchange）に基づいて通信相手端末６との間で鍵交換処理を実行し，この処理により決定された暗号鍵（共通鍵，秘密鍵等）を加入者端末５に与える。

【００３１】

認証サーバ３は，本実施の形態では，サービス管理サーバを兼ねており，加入者端末５等の認証データに加えて，後に詳述するサービスプロファイル（原本）を保持する。そして，認証サーバ３は，加入者端末５のネットワーク接続の際の認証を契機としてサービスプロファイル（コピー）をサービス制御装置１に送信する。

【００３２】

なお，サービスプロファイルは，認証サーバ３に連携した図示しないデータベ

ースに格納されてもよい。また，認証サーバ３とサービス管理サーバとは，個別に設けられてもよい。両サーバが個別に設けられる場合には，サービスプロファイルは，サービス管理サーバからサービス制御装置１に転送されることとなる。

【００３３】

図１では，理解を容易にするために１つのサービス制御装置１を示しているが，コアネットワーク７には複数のサービス制御装置が存在し，加入者端末５は，その移動に伴って，一般に，最寄りのサービス制御装置と無線接続を確立する。鍵交換代理サーバもコアネットワーク７に複数存在してもよい。サービス制御装置および鍵交換代理サーバが複数存在する場合には，各サービス制御装置は，自己の最寄りの鍵交換代理サーバのＩＰアドレスを知り，最寄りの鍵交換代理サーバに加入者端末５の鍵交換処理を代理させることとなる。

【００３４】

図２は，サービス制御装置１の構成を示すブロック図である。サービス制御装置１は，メッセージ送受信部１１，プロトコル制御部１２，およびサービス管理部１３を有する。

【００３５】

メッセージ送受信部１１は，コアネットワーク７に接続され，コアネットワーク７を介して加入者端末５，鍵交換代理サーバ２，認証サーバ３，ルータ４等からのパケット（以下「メッセージ」ともいう。）を受信し，これらの端末，サーバ，ルータ等にメッセージを送信する。

【００３６】

プロトコル制御部１２は，メッセージ送受信部１１が受信したメッセージを受け取り，メッセージを解析する。そして，プロトコル制御部１２は，メッセージの解析によりメッセージを転送するかどうか，および，転送する場合の転送先を決定するとともに，必要に応じてメッセージのカプセル化等を行う。

【００３７】

このメッセージを転送するかどうかを判断するために，プロトコル制御部１２は，認証サーバ３から与えられたサービスプロファイルを保持する。図３は，サービスプロファイルの一例を示している。

【００３８】

サービスプロファイルは，ネットワーク運用者と加入者との契約に基づいて作成されるファイルであり，加入者端末（加入者）ごとに設けられる。各加入者のサービスプロファイルは，加入者識別情報および１または２以上のＩＰＳｅｃ適用条件を有する。

【００３９】

加入者識別情報は，加入者（加入者端末）を識別するための情報であり，たとえば電話番号，ＮＡＩ（Network Access ID），認証データベースのエントリ番号等のデータ項目を有する。

【００４０】

ＩＰＳｅｃ適用条件は，（１）通信相手端末６から加入者端末５宛てに送信されるメッセージのうち，鍵交換代理サーバ２に転送するメッセージの条件，（２）加入者端末５から通信相手端末６宛てに送信されたメッセージのうち，鍵交換代理サーバ２に転送するメッセージの条件，または，（３）サービス制御装置１宛てに送信されたメッセージのうち，加入者端末５もしくは通信相手端末６に転送するメッセージの条件を規定したデータである。

【００４１】

このＩＰＳｅｃ適用条件は，ＩＰアドレスおよびポート番号を有する。「ＩＰアドレス」は，上記（１）～（３）の転送すべきメッセージが有する宛先ＩＰアドレスまたは送信元ＩＰアドレスを示す。「ポート番号」は，ＴＣＰやＵＤＰにおけるアプリケーションを指定する番号であり，たとえば後述する鍵交換メッセージ（ＩＫＥメッセージ）には，ポート番号として５００番が使用される

サービス制御装置１は，受信したメッセージの宛先ＩＰアドレスまたは送信元ＩＰアドレスとＩＰＳｅｃ適用条件のＩＰアドレスとが一致するかどうか，および，受信したメッセージのポート番号がＩＰＳｅｃ適用条件のポート番号とが一致するかどうかを判断し，一致する場合にはそのメッセージの内容に応じて，そのメッセージを鍵交換代理サーバ２，加入者端末５，または通信相手端末６に転送する。

【００４２】

転送されるメッセージは，本実施の形態では，後述するように，（１）加入者端末５から通信相手端末６宛てに送信される鍵交換メッセージ（鍵交換代理要求メッセージ）（転送先：鍵交換代理サーバ２），（２）通信相手端末６から加入者端末５宛てに送信される鍵交換メッセージ（転送先：鍵交換代理サーバ２），（３）鍵交換代理サーバ２からサービス制御装置１宛てに送信された鍵交換メッセージ（転送先：通信相手端末６），（４）鍵交換代理サーバ２からサービス制御装置１宛てに送信された鍵情報（ＳＡデータ）を含むメッセージ（転送先：加入者端末５）である。

【００４３】

なお，ＩＰＳｅｃ適用条件の「ＩＰアドレス」は，たとえば加入者端末５と通信する通信相手端末（通信相手端末６等）の双方のＩＰアドレスの組を示す場合もある。

【００４４】

サービスプロファイルは，加入者端末５が位置登録をし，認証サーバ３によって認証された時に，認証サーバ（すなわちサービス管理サーバ）３からサービス制御装置１に送信され，保持される。したがって，加入者端末５が移動し，アクセスするサービス制御装置１が変化すると，アクセスされるサービス制御装置１に認証サーバ３からサービスプロファイルが送信されることとなる。

【００４５】

図２に戻って，サービス管理部１３は，プロトコル管理部１２のメッセージの解析結果を受け取り，メッセージに対して行った処理等のサービスの管理する。

【００４６】

図４は，加入者端末５の構成を示すブロック図である。加入者端末５は，アプリケーション処理部５１，メッセージ送受信部５２，暗号化／復号化部５３，プロトコル制御部５４，および暗号処理管理部５５を有する。

【００４７】

アプリケーション処理部５１は，たとえばブラウザ，メーラ等のアプリケーションプログラムを実行し，ユーザとのインタフェース処理を実行する。そして，アプリケーション処理部５１は，ユーザの入力に基づいて，メッセージ送受信部

５２にメッセージ送信要求を与えるとともに，メッセージ送受信部５２により受信されたメッセージに含まれるデータを表示装置等に出力，表示等する。

【００４８】

メッセージ送受信部５２は，コアネットワーク７に接続され，コアネットワーク７を介してサービス制御装置１からのメッセージを受信し，サービス制御装置１にメッセージを送信する。

【００４９】

暗号化／復号化部５３は，送信メッセージの暗号化および受信メッセージの復号化を行う。プロトコル制御部５４は，通信相手端末６との通信に必要な鍵が存在しない場合には，鍵交換メッセージ（鍵交換代理要求メッセージ）を生成し，また，セキュリティアソシエーション（ＳＡ：Security Association）データを含むメッセージ（鍵メッセージ）を鍵交換代理サーバ２から受信した場合には，受信メッセージからＳＡデータを抽出する。

【００５０】

暗号処理管理部５５は，セキュリティポリシーデータベース（ＳＰＤ：Security Policy Database）およびセキュリティアソシエーションデータベース（ＳＡＤ：Security Association Database）を保持し，これらのデータに基づいて通信相手端末６との通信に暗号化が必要かどうかや鍵の有無を判断する。

【００５１】

図５（Ａ）は，加入者端末５の暗号処理管理部５５に保持されるＳＰＤを示し，同図（Ｂ）は加入者端末５の暗号処理管理部５５に保持されるＳＡＤを示している。

【００５２】

ＳＰＤは，加入者端末５にＩＰＳｅｃによる暗号化通信を適用するための１または２以上のＩＰＳｅｃ適用条件を含んでいる。各ＩＰＳｅｃ適用条件は，その内容として，前述したサービスプロファイル（図３参照）と同様に，ＩＰアドレスおよびポート番号を有する。「ＩＰアドレス」は，暗号化通信が必要とされる通信相手端末のＩＰアドレスであり，「ポート番号」は，暗号化通信が必要されるポート番号（ＴＣＰやＵＤＰにおけるアプリケーションを指定する番号）であ

る。

【００５３】

加入者端末５がこれらＩＰアドレスおよびポート番号と一致するパケットを送信する場合に，その送信パケットにはＩＰＳｅｃ／ＩＫＥによる暗号化通信が適用される。

【００５４】

ＳＡＤは，１または２以上のセキュリティアソシエーションデータ（ＳＡデータ）からなる。各ＳＡデータは，適用条件および内容を有する。「適用条件」は，ＳＰＤの適用条件と同様のＩＰアドレスおよびポート番号を有する。「内容」は，暗号化通信に使用される暗号化方法（暗号化プロトコル，たとえばＤＥＳ等），暗号化に使用される鍵（暗号鍵），およびＳＰＩ（Security Parameter Index）のデータ項目を含んでいる。「ＳＰＩ」は暗号化されたメッセージに付与され，受信側は，このＳＰＩにより暗号プロトコルおよび鍵を特定し，受信したメッセージを復号化する。

【００５５】

加入者端末５の暗号処理管理部５５は，ＳＰＤのＩＰアドレスおよびポート番号とそれぞれ一致するＩＰアドレスおよびポート番号を有するＳＡデータがＳＡＤに存在するかどうかを判断し，存在する場合には，その暗号化プロトコルおよび鍵を使用してメッセージを暗号化して送信し，存在しない場合には，存在しない旨をプロトコル制御部５４に通知する。

【００５６】

図６は，鍵交換代理サーバ２の構成を示すブロック図である。鍵交換代理サーバ２は，メッセージ送受信部２１，プロトコル制御部２２，および鍵生成部２３を有する。

【００５７】

メッセージ送受信部２１は，コアネットワーク７に接続され，コアネットワーク７を介してサービス制御装置１からのメッセージを受信し，サービス制御装置１にメッセージを送信する。

【００５８】

プロトコル制御部２２は，メッセージ送受信部２１により受信されたメッセージの解析，通信相手端末６と鍵交換処理（鍵交換プロセス）を実行し，決定された鍵をメッセージ送受信部２１に与える。

【００５９】

鍵生成部２３は，プロトコル制御部２２により実行される鍵交換プロセスにおいて，プロトコル制御部２２の要求に応じて鍵を生成する。この鍵の生成において，たとえばべき乗計算が行われる。

【００６０】

次に，この鍵交換代理ネットワークシステムにおける鍵交換代理処理の流れを説明する。

【００６１】

図７は，加入者端末５による鍵交換メッセージ（鍵交換代理要求メッセージ）の送信から，加入者端末５と通信相手端末６との間で暗号化通信が行われるまでの全体のメッセージの流れを示している。図８は，加入者端末５の詳細な処理の流れを示すシーケンス図である。図９は，サービス制御装置１の詳細な処理の流れを示すシーケンス図である。図１０は，図９のステップＳ１２の詳細な処理の流れを示すフローチャートである。図１１は，鍵交換代理サーバ２の詳細な処理の流れを示すシーケンス図である。

【００６２】

まず，図８を参照して，加入者端末５のメッセージ送受信部５２は，アプリケーション処理部５１（図８には図示略）から与えられた通信相手端末６宛てのパケット送信要求（メッセージ送信要求）により，パケット送信を検出する（Ｓ１）。メッセージ送受信部５２は，パケット送信を検出すると，パケットの暗号化の必要の有無および鍵（暗号鍵）の有無を暗号処理管理部５５に問い合わせる。

【００６３】

暗号処理管理部５５は，メッセージ送受信部５２の問合せにより，送信パケットのＩＰアドレス（宛先アドレス）およびポート番号とそれぞれ一致するＩＰアドレスおよびポート番号を有するＩＰＳｅｃ適用条件がＳＰＤに存在するかどうかを判断する。一致するＩＰＳｅｃ適用条件が存在する場合には，暗号処理管理

部５５は，送信パケットの暗号化が必要であると判断し，続いて，ＩＰアドレスおよびポート番号とそれぞれ一致するＳＡデータがＳＡＤに存在するかどうかを判断する。一方，一致するＩＰＳｅｃ適用条件が存在しない場合には，暗号処理管理部５５は上記処理を実行せず，送信パケットは通常のＩＰプロトコルに従って宛先アドレスが示す通信相手端末６に送信される。

【００６４】

暗号化が必要であると判断された場合において，一致するＳＡデータがＳＡＤに存在しないときは，暗号処理管理部５５は，鍵が存在しないことをプロトコル制御部５４に通知する。この通知により，プロトコル制御部５４は，鍵交換メッセージ（鍵交換代理要求メッセージ）を作成し，メッセージ送受信部５２に与える。

【００６５】

メッセージ送受信部５２は，与えられた鍵交換メッセージをサービス制御装置１（メッセージの宛先は通信相手端末６）に送信する。この鍵交換メッセージの送信は，図７において符号（１）の破線の矢印で示される。

【００６６】

なお，暗号化が必要であると判断された場合において，一致するＳＡデータがＳＡＤに存在するときの処理については，後の図１５に従って説明する。

【００６７】

図１２（Ａ）は，加入者端末５からサービス制御装置１に送信される鍵交換メッセージ（鍵交換代理要求メッセージ）の構成を示している。この鍵交換メッセージは，ＩＰヘッダ（ヘッダ部）およびデータ部を有する。

【００６８】

ＩＰヘッダには，送信元アドレスＳＡとして加入者端末５のＩＰアドレスが，宛先アドレスＤＡとして通信相手端末６のＩＰアドレスが，それぞれ含まれる。すなわち，加入者端末５は，あくまで通信相手端末６と通信を行うものと認識している。

【００６９】

データ部には，ＵＤＰヘッダおよびＩＫＥヘッダが含まれ，ＵＤＰヘッダには

，ＩＰＳｅｃ／ＩＫＥにおける鍵交換メッセージで通常使用されるＵＤＰ（User Datagram Protocol）の５００番のポート番号が設定される。ＩＫＥヘッダにはクッキー（Cookie）が含まれ，このクッキーには特殊な値（タイプ値）が設定される。特殊な値として，たとえば上位および下位の８バイトとも１００が設定される。通常のメッセージでは，上位８バイトを送信者が決定し，下位８バイトを応答者が決定するために，この特殊な値を鍵交換代理サーバ２に予約しておくことにより，メッセージの識別が可能となる。なお，ＵＤＰの値には，５００番以外の値を使用することもできる。

【００７０】

続いて，図９を参照して，サービス制御装置１のメッセージ送受信部１１は，加入者端末５から鍵交換メッセージを受信すると，受信したメッセージをプロトコル制御部１２に与える。

【００７１】

プロトコル制御部１２は，メッセージ送受信部１１からメッセージを受け取ると，サービスプロファイル（図３参照）に基づいてメッセージ解析処理を実行する（Ｓ１２）。

【００７２】

このメッセージ解析処理において，プロトコル制御部１２は，図１０に示すように，まず受信パケット（メッセージ）が加入者端末５から送信された鍵交換メッセージかどうかを判断する（Ｓ２１）。この判断は，受信パケットの送信元アドレスＳＡ（すなわち加入者端末５のＩＰアドレス）と鍵交換メッセージに含まれるポート番号（すなわちＵＤＰの５００番）とが，サービスプロファイルのＩＰＳｅｃ適用条件に存在するかどうかと，受信パケットの内容に基づいて行われる。

【００７３】

プロトコル制御部１２は，送信元アドレスおよびポート番号がサービスプロファイルのＩＰＳｅｃ適用条件に存在する場合には（Ｓ２１でＹ），受信パケットの内容に基づいて，その受信メッセージが鍵交換代理要求メッセージ，鍵交換メッセージ（ＩＫＥメッセージ），または加入者端末５宛ての鍵情報（ＳＡデータ

）を含むメッセージ（鍵転送メッセージ）のいずれであるかを判断する。

【００７４】

たとえば，受信パケットにＵＤＰヘッダやＩＫＥヘッダが含まれている場合には，その受信パケットが鍵交換代理要求メッセージまたは鍵交換メッセージであると判断できる。鍵転送メッセージには，ＳＡデータ等が含まれていることから，受信パケットが鍵転送メッセージであると判断できる。

【００７５】

そして，受信パケットが鍵交換代理要求メッセージである場合には（Ｓ２１でＹ），プロトコル制御部１２は，メッセージ送受信部１１を介して，受信パケット（すなわち鍵交換代理要求メッセージ）を鍵交換代理サーバ２に転送する（Ｓ２６，図９のＳ１３）。

【００７６】

受信パケットが鍵交換メッセージである場合には（Ｓ２２でＹ），プロトコル制御部１２は，メッセージ送受信部１１を介して，受信パケット（すなわち鍵交換メッセージ）を，その受信パケットの送信元アドレスまたは宛先アドレスに基づいて，鍵交換代理サーバ２または通信相手端末６に転送する（Ｓ２６，図９のＳ１３）。たとえば，受信パケットの送信元アドレスが通信相手端末６の場合には，受信パケットは鍵交換代理サーバ２に転送される。受信パケットの送信元アドレスが鍵交換代理サーバ２の場合には，受信パケットは通信相手端末６に転送される。

【００７７】

受信パケットが加入者宛ての鍵情報（ＳＡ）を含むメッセージである場合には（Ｓ２３でＹ），プロトコル制御部１２は，メッセージ送受信部１１を介して，受信パケットを加入者端末５に転送する（Ｓ２５，図９のＳ１３）。

【００７８】

受信パケットが鍵交換代理要求メッセージ，鍵交換メッセージ，および加入者宛ての鍵情報を含むメッセージのいずれでもない場合には（Ｓ２１～Ｓ２３でＮ），プロトコル制御部１２は通常のルーティングにしたがって受信パケットをルータ，端末等に転送する（Ｓ２４，図９のＳ１３）。

【００７９】

このようにして，加入者端末５からサービス制御装置１に送信された鍵交換代理要求メッセージは，サービス制御装置１から鍵交換代理サーバ２に転送される。

【００８０】

図１２（Ｂ）は，サービス制御装置１から鍵交換代理サーバ２に転送される鍵交換代理要求メッセージの構成を示している。サービス制御装置１のプロトコル制御部１２またはメッセージ送受信部１１は，加入者端末５から送信された鍵交換代理要求メッセージをカプセル化し，新たなＩＰパケットのデータ部に組み込む。そして，この新たなＩＰパケットのＩＰヘッダには，送信元アドレスとしてサービス制御装置１のＩＰアドレスが書き込まれ，宛先アドレスとして鍵交換代理サーバ２のＩＰアドレスが書き込まれる。

【００８１】

続いて，図１１を参照して，鍵交換代理サーバ２のメッセージ送受信部２１は，サービス制御装置１から，図１２（Ｂ）に示す鍵交換代理要求メッセージを受信すると（Ｓ３１），受信メッセージをプロトコル制御部２２に与える。

【００８２】

プロトコル制御部２２は，受信メッセージを解析し（Ｓ３２），受信メッセージが鍵交換代理要求メッセージであると判断すると，データ部にカプセル化された鍵交換代理要求メッセージの宛先アドレスＤＡ（図１２（Ｂ）参照）に基づいて通信相手（ここでは通信相手端末６）を特定する。そして，プロトコル制御部２２は，特定した通信相手である通信相手端末６との間でＩＰＳｅｃ／ＩＫＥに基づく鍵交換プロセスを実行する（Ｓ３２）。この鍵交換プロセスにおいて，プロトコル制御部２２は，必要に応じて鍵生成部２３に鍵の生成を依頼し，この依頼に応じて，鍵生成部２３は鍵を生成する。

【００８３】

プロトコル制御部２２は，鍵交換プロセスにおいて，通信相手端末６に送信する鍵交換メッセージ（ＩＫＥメッセージ）を作成する（Ｓ３４）。図１３（Ｄ）は，鍵交換代理サーバ２のプロトコル制御部２２により作成される鍵交換メッセ

ージの構成を示している。

【００８４】

鍵交換代理サーバ２は，加入者端末５の鍵交換処理を代理するものであるので，鍵交換代理サーバ２が作成する鍵交換メッセージのデータ部には，加入者端末５と通信相手端末６との間で交換される鍵交換メッセージ（ＩＫＥメッセージ）がカプセル化される。すなわち，データ部に含まれる鍵交換メッセージの送信元アドレスＳＡは加入者端末５のＩＰアドレスとなり，宛先アドレスＤＡは通信相手端末６のＩＰアドレスとなる。また，ＩＰヘッダには，送信元アドレスＳＡとして鍵交換代理サーバ２のＩＰアドレスと，宛先アドレスＤＡとしてサービス制御装置１のＩＰアドレスが含まれる。なお，図１３（Ｄ）に示す鍵交換メッセージのデータ部にカプセル化された鍵交換メッセージは，図１２（Ａ）に示す鍵交換メッセージ（鍵交換代理要求メッセージ）と同じ構造を有する。

【００８５】

図１１に戻って，図１３（Ｄ）に示す鍵交換メッセージは，プロトコル制御部２２からメッセージ送受信部２１に与えられ，メッセージ送受信部２１からサービス制御装置１に送信される（Ｓ３５）。

【００８６】

図９および図１０を再び参照して，鍵交換代理サーバ２からサービス制御装置１に送信された鍵交換メッセージ（図１３（Ｄ）参照）は，サービス制御装置１による前述した図１０のステップＳ２２およびＳ２６の処理にしたがって通信相手端末６に転送される。この際，鍵交換代理サーバ２からサービス制御装置１に送信された鍵交換メッセージは，カプセル化が解除され，データ部にカプセル化された鍵交換メッセージが取り出される。図１３（Ａ）は，データ部から取り出されたメッセージの構成を示している。

【００８７】

この取り出されたメッセージは，その宛先アドレスＤＡ（すなわち通信相手端末６のＩＰアドレス）に基づいて，サービス制御装置１から通信相手端末６に送信される。

【００８８】

通信相手端末６は，図１３（Ａ）に示す鍵交換メッセージを受信すると，鍵交換代理サーバ２と同様にＩＰＳｅｃ／ＩＫＥによる鍵交換プロセスを実行する。ここで，通信相手端末６が受信する鍵交換メッセージは図１３（Ａ）に示すものであるので，通信相手端末６は，鍵交換代理サーバ２ではなく，加入者端末５から鍵交換メッセージを受信したものと認識し，加入者端末５と鍵交換を行っていると判断する。

【００８９】

したがって，鍵交換プロセスにおいて通信相手端末６が送信する鍵交換メッセージは，図１３（Ｂ）に示すように，送信元アドレスＳＡとして通信相手端末６のＩＰアドレスを有し，宛先アドレスＤＡとして加入者端末５のＩＰアドレスを有するメッセージとなる。

【００９０】

加入者端末５は，前述したように，サービス制御装置１と無線接続しているので，加入者端末５宛てに送信されるメッセージは，すべてサービス制御装置１を通過する。したがって，通信相手端末６から加入者端末５宛てに送信された鍵交換メッセージ（図１３（Ｂ）参照）は，サービス制御装置１に受信される。

【００９１】

サービス制御装置１は，前述した図１０に示すステップＳ２２およびＳ２６の処理により，通信相手端末６から加入者端末５宛てに送信された鍵交換メッセージを鍵交換代理サーバ２に転送する。この際，この鍵交換メッセージは，図１３（Ｃ）に示すようにカプセル化される。すなわち，通信相手端末６から送信された鍵交換メッセージがデータ部にカプセル化され，ＩＰヘッダの送信元アドレスＳＡはサービス制御装置１のＩＰアドレスとされ，宛先アドレスＤＡは鍵交換代理サーバ２のＩＰアドレスとされる。

【００９２】

図１１に戻って，この図１３（Ｃ）に示す鍵交換メッセージは，鍵交換代理サーバ２に受信され（Ｓ３１），メッセージ解析された後（Ｓ３２），鍵交換プロセスに従って処理される（Ｓ３３）。

【００９３】

このような処理が行われ，鍵交換代理サーバ２と通信相手端末６との間で鍵（暗号鍵）が決定される。このような鍵交換代理サーバ２と通信相手端末６との間における鍵交換メッセージの送受信は，図７の符号（２）の矢印で示される。

【００９４】

鍵が決定されると，鍵交換代理サーバ２のプロトコル制御部２２は，決定された鍵を鍵転送メッセージによりサービス制御装置１に送信する（Ｓ３４，Ｓ３５）。図１４（Ａ）は，鍵交換代理サーバ２からサービス制御装置１に送信される鍵転送メッセージの構成を示している。

【００９５】

この鍵転送メッセージのＩＰヘッダには，送信元アドレスとして鍵交換代理サーバ２のＩＰアドレスが含まれ，宛先アドレスとしてサービス制御装置１のＩＰアドレスが含まれている。データ部には，鍵情報（ＳＡデータ）を含む鍵メッセージがカプセル化されている。

【００９６】

鍵の交換は，鍵交換代理サーバ２が加入者端末５に代理して行っているものの，加入者端末５と通信相手端末６との間で行われたことになっている。したがって，カプセル化された鍵メッセージのＩＰヘッダには，送信元アドレスＳＡとして通信相手端末６のＩＰアドレスが含まれ，宛先アドレスＤＡとして加入者端末５のＩＰアドレスが含まれる。

【００９７】

鍵メッセージのデータ部には，鍵情報（すなわち図５（Ｂ）に示すＳＡデータ）が含まれている。

【００９８】

鍵転送メッセージが鍵交換代理サーバ２からサービス制御装置１に送信されると，サービス制御装置１は，前述した図１０のステップＳ２３およびＳ２５の処理により，鍵転送メッセージを加入者端末５に送信する。図１４（Ｂ）は，サービス制御装置１から加入者端末５に送信される鍵転送メッセージの構成を示している。

【００９９】

この鍵転送メッセージは，前述した図１４（Ａ）に示すものとほぼ同じであるが，ＩＰヘッダの送信元アドレスＳＡおよび宛先アドレスＤＡが異なる。送信元アドレスＳＡはサービス制御装置１のＩＰアドレスとされ，宛先アドレスＤＡは加入者端末５のＩＰアドレスとされる。

【０１００】

鍵交換代理サーバ２からサービス制御装置１を介して加入者端末５に送信される鍵転送メッセージの流れは，図７の符号（３）の矢印により示される。

【０１０１】

図８に戻って，加入者端末５のメッセージ送受信部５２は，サービス制御装置１から鍵転送メッセージを受信すると（Ｓ５），カプセル化を解除して，データ部に含まれる鍵メッセージをプロトコル制御部５４に与える。

【０１０２】

プロトコル制御部５４は，鍵メッセージに含まれる鍵情報（ＳＡデータ）を抽出し，ＳＡデータを暗号処理管理部５５に与える（Ｓ６）。暗号処理管理部５５は，プロトコル制御部５４から受け取ったＳＡデータをＳＡＤに追加する（Ｓ７）。

【０１０３】

以後，加入者端末５は，このＳＡデータに含まれる鍵および暗号化プロトコルに従ってデータを暗号化し，暗号化されたデータを通信相手端末６に送信する。図１５は，鍵が決定された後の加入者端末５のパケットの送受信処理の流れを示すシーケンス図である。

【０１０４】

加入者端末５のアプリケーション処理部５１が通信相手端末６宛てのパケット送信要求をメッセージ送受信部５２に与えると，メッセージ送受信部５２は，パケット送信を検出し（Ｓ４１），パケットの暗号化の必要の有無および鍵の有無を暗号処理管理部５５に問い合わせる。暗号処理管理部５５は，ＳＰＤおよびＳＡＤ（図５（Ａ）および（Ｂ）参照）により暗号化の必要の有無および鍵の有無を判断する（Ｓ４２）。これらの処理は，前述した図８のステップＳ１およびＳ２の処理と同じである。

【０１０５】

ここでは，暗号化が必要であり，かつ，鍵が存在するものとする。この場合に，暗号処理管理部５５は，ＳＰＤのＩＰアドレスおよびポート番号にそれぞれ一致するＩＰアドレスおよびポート番号を有するＳＡデータを選択し（Ｓ４３），選択したＳＡデータに基づく暗号化処理を暗号化／復号化部５３に指示する。

【０１０６】

暗号化／復号化部５３は，この指示により，選択されたＳＡデータの鍵および暗号化プロトコルを使用してパケットを暗号化する（Ｓ４４）。また，暗号化／復号化部５３は，選択されたＳＡデータに含まれるＳＰＩを暗号化されたパケットの所定のフィールドに書き込む。

【０１０７】

この暗号化されたパケットは，メッセージ送受信部５２に与えられ，メッセージ送受信部５２からサービス制御装置１に送信される（Ｓ４５）。サービス制御装置１は，このパケットを図１０のステップＳ２４の通常ルーティング処理により転送する。これにより，このパケットは，サービス制御装置１からルータ４を介して通信相手端末６に送信される。このパケットの送信は，図７の符号（４）の矢印により示される。

【０１０８】

通信相手端末６は，暗号化されたパケットを受信すると，パケットに含まれるＳＰＩおよび保持するＳＡＤに基づいて，鍵および暗号化プロトコルを特定し，特定した鍵および暗号化プロトコルに基づいてパケットを復号化する。

【０１０９】

一方，通信相手端末６から加入者端末５に暗号化パケットが送信されると，この暗号化パケットは，ルータ４およびサービス制御装置１を介して加入者端末５のメッセージ送受信部５２に受信される（Ｓ４６）。このパケットの送信も，図７の符号（４）の矢印により示される。

【０１１０】

メッセージ送受信部５２は，受信したパケットを暗号化／復号化部５３に与える。暗号化／復号化部５３は，パケットに含まれるＳＰＩを暗号処理管理部５５

に与える。暗号処理管理部５５は，暗号化／復号化部５３から与えられたＳＰＩと一致するＳＡデータをＳＡＤから検索および抽出し（Ｓ４７），抽出したＳＡデータの鍵および暗号化プロトコル（復号化プロトコル）を暗号化／復号化部５３に与える。

【０１１１】

暗号化／復号化部５３は，暗号処理管理部５５から与えられた鍵および暗号化プロトコルに従ってパケットを復号化する（Ｓ４８）。

【０１１２】

このようにして，加入者端末５と通信相手端末６との間で，暗号化通信が行われる。

【０１１３】

次に，通信相手端末６から加入者端末５宛てに，ＩＰＳｅｃ／ＩＫＥに基づく鍵交換要求が送信された場合の処理について説明する。

【０１１４】

図１６は，通信相手端末６による鍵交換メッセージの送信から，通信相手端末６と加入者端末５との間で暗号化通信が行われるまでの全体のメッセージの流れを示している。

【０１１５】

通信相手端末６においても，加入者端末５と同様にして，加入者端末５宛てのパケットの暗号化の必要の有無および鍵の有無がＳＰＤおよびＳＡＤに基づいて判断される。そして，暗号化が必要と判断されたが，鍵（および暗号化プロトコル）を規定したＳＡデータが存在しない場合には，通信相手端末６は，前述した図１３（Ｂ）に示す鍵交換メッセージを加入者端末５宛てに送信する。

【０１１６】

この鍵交換メッセージは，その宛先アドレスＤＡが加入者端末５のＩＰアドレスであるので，サービス制御装置１に受信される。サービス制御装置１は，図１０のステップＳ２２およびＳ２６の処理に従って，鍵交換メッセージを図１３（Ｃ）に示すようにカプセル化し，カプセル化後の鍵交換メッセージを鍵交換代理サーバ２に転送する。この鍵交換メッセージの流れが図１６の符号（１）の矢印

で示されている。

【０１１７】

その後，前述と同様にして，鍵交換代理サーバ２と通信相手端末６との間で，鍵交換プロセスに従って鍵交換メッセージが交換され，鍵が決定される。この鍵交換メッセージの交換は，図１６の符号（２）の矢印で示されている。

【０１１８】

鍵交換代理サーバ２と通信相手端末６との間で鍵が決定されると，決定された鍵は，図１４（Ａ）に示す鍵転送メッセージとして鍵交換代理サーバ２からサービス制御装置１に送信され，さらに，図１４（Ｂ）に示す鍵転送メッセージとしてサービス制御装置１から加入者端末５に送信される。この鍵転送メッセージの流れが図１６の符号（３）の矢印で示されている。

【０１１９】

加入者端末５は，鍵転送メッセージを受信すると，前述したのと同様に，鍵転送メッセージに含まれるＳＡデータをＳＡＤに追加する。その後，加入者端末５は，通信相手端末６から送信されてきた暗号化パケットをＳＡＤに基づいて復号化し，また，通信相手端末６宛てに送信するパケットをＳＡＤに基づいて暗号化して送信する。この通信相手端末６と加入者端末５との間の暗号化パケットの送受信が図１６の符号（４）の矢印で示されている。

【０１２０】

このように，本発明の実施の形態によると，ＩＰＳｅｃ／ＩＫＥに基づく鍵交換処理を，鍵交換代理サーバ２が加入者端末５に代わって通信相手端末６との間で実行する。したがって，加入者端末５がＩＰＳｅｃ／ＩＫＥによる鍵交換処理を行う必要はないので，加入者端末５の処理が軽減される。また，加入者端末５は鍵交換処理のプログラム（鍵交換サーバ）を保持する必要はないので，加入者端末５のメモリ容量を小さくすることができ，その結果，装置の小型軽量化および装置コストの低減を図ることができる。さらに，鍵交換サーバの実行に伴う電力消費もないので，加入者端末５の省電力化に貢献する。

【０１２１】

また，本発明の実施の形態によると，サービス制御装置１が，鍵交換代理サー

バ２の位置（ＩＰアドレス）を知り，サービスプロファイルに基づいて鍵交換代理サーバ２へのメッセージ転送の必要の有無を判断する。したがって，加入者端末５および通信相手端末６は，ともに鍵交換代理サーバ２の位置を知る必要はなく，知らなくても鍵交換を行い，その後の暗号化通信を行うことができる。

【０１２２】

なお，通信相手端末６も，加入者端末５と同様に，鍵交換サーバを有しない携帯端末等の場合もある。この場合には，通信相手端末６がアクセスするルータ４がサービス制御装置となり，また，このサービス制御装置の最寄りの鍵交換代理サーバが通信相手端末６に代わって鍵交換処理を行う。そして，加入者端末５の鍵交換代理サーバ２と通信相手端末６の鍵交換代理サーバとの間で鍵交換処理が実行され，決定された鍵が，それぞれの鍵交換代理サーバから加入者端末５および通信相手端末６にそれぞれ送信される。

【０１２３】

また，このように，通信相手端末６について，鍵交換代理サーバが鍵交換を代行する場合に，この鍵交換代理サーバは，加入者端末５の鍵交換を代行する鍵交換代理サーバと同一のサーバであってもよい。同様にして，通信相手端末６のメッセージ転送を行うサービス制御装置も，サービス制御装置１と同一であってもよい。

【０１２４】

コアネットワーク７の運用者には，特定のアクセス手段を所有せず，大規模ネットワークの運用者からネットワーク（の一部）を借りて，利用者にサービスを提供するＭＮＶＯ（Mobile Virtual Network Operator）も含まれる。

【０１２５】

（付記１）　暗号通信を行う第１および第２の端末装置の間で行われる鍵交換処理を代行する鍵交換代理ネットワークシステムであって，

前記第１の端末装置にアクセスされる第１のサービス制御装置および前記第１の端末装置の鍵交換処理を代行する第１の鍵交換代理装置を備え，

前記第１のサービス制御装置は，

前記第１もしくは第２の端末装置または前記第１の鍵交換代理装置からのメッ

セージを受信する第１のメッセージ受信部と，

前記第１のメッセージ受信部により受信されたメッセージが鍵交換メッセージまたは鍵を含むメッセージかどうかを判断するための第１のデータを保持し，該第１のデータに基づいて前記受信メッセージが前記鍵交換メッセージまたは前記鍵を含むメッセージかどうかを判断し，前記受信メッセージが前記第１または第２の端末装置からの鍵交換メッセージの場合には転送先を前記第１の鍵交換代理装置とし，前記受信メッセージが前記第１の鍵交換代理装置からの鍵交換メッセージの場合には転送先を前記第２の端末装置とし，前記受信メッセージが前記鍵を含むメッセージの場合には転送先を前記第１の端末装置として決定する第１のプロトコル制御部と，

前記第１のプロトコル制御部により決定された転送先に前記第１のメッセージ受信部により受信されたメッセージを送信する第１のメッセージ送信部と，

を備え，

前記第１の鍵交換代理装置は，

前記第１のサービス制御装置からのメッセージを受信する第２のメッセージ受信部と，

前記第２のメッセージ受信部により受信されたメッセージが前記鍵交換メッセージである場合に，前記第２の端末装置との間で前記鍵交換メッセージを交換して鍵を決定する第２のプロトコル制御部と，

前記第２のプロトコル制御部により決定された前記鍵を，前記鍵を含むメッセージとして前記第１のサービス制御装置宛てに送信する第２のメッセージ送信部と，

を備えている鍵交換代理ネットワークシステム。

【０１２６】

（付記２）　付記１において，

前記第２のプロトコル制御部は，前記第１の端末装置からの鍵交換メッセージの受信を契機として前記第２の端末装置との間で鍵を決定する，鍵交換ネットワークシステム。

【０１２７】

（付記３）　付記１において，

前記第２のプロトコル制御部は，前記第２の端末装置からの鍵交換メッセージの受信を契機として前記第２の端末装置との間で鍵を決定する，鍵交換ネットワークシステム。

【０１２８】

（付記４）　付記１から３のいずれか１つにおいて，

前記第２の端末装置にアクセスされる第２のサービス制御装置および前記第２の端末装置の鍵交換処理を代行する第２の鍵交換代理装置をさらに備え，

前記第２のサービス制御装置は，

前記第１もしくは第２の端末装置または前記第２の鍵交換代理装置からのメッセージを受信する第３のメッセージ受信部と，

前記第３のメッセージ受信部により受信されたメッセージが鍵交換メッセージまたは鍵を含むメッセージかどうかを判断するための第２のデータを保持し，該第２のデータに基づいて前記受信メッセージが前記鍵交換メッセージまたは前記鍵を含むメッセージかどうかを判断し，前記受信メッセージが前記第１または第２の端末装置からの鍵交換メッセージの場合には転送先を前記第２の鍵交換代理装置とし，前記受信メッセージが前記第２の鍵交換代理装置からの鍵交換メッセージの場合には転送先を前記第１の端末装置とし，前記受信メッセージが前記鍵を含むメッセージの場合には転送先を前記第２の端末装置として決定する第３のプロトコル制御部と，

前記第３のプロトコル制御部により決定された転送先に前記第３のメッセージ受信部により受信されたメッセージを送信する第３のメッセージ送信部と，

を備え，

前記第２の鍵交換代理装置は，

前記第２のサービス制御装置からのメッセージを受信する第４のメッセージ受信部と，

前記第４のメッセージ受信部により受信されたメッセージが前記鍵交換メッセージである場合に，前記第１の鍵交換代理装置との間で前記鍵交換メッセージを交換して鍵を決定する第４のプロトコル制御部と，

前記第４のプロトコル制御部により決定された前記鍵を，前記鍵を含むメッセージとして前記第２のサービス制御装置宛てに送信する第４のメッセージ送信部と，

を備えている鍵交換代理ネットワークシステム。

【０１２９】

（付記５）　付記４において，

前記第１および第２のサービス制御装置が同一の装置により構成される，鍵交換代理ネットワークシステム。

【０１３０】

（付記６）　付記４または５において，

前記第１および第２の鍵交換代理装置が同一の装置により構成される，鍵交換代理ネットワークシステム。

【０１３１】

（付記７）　端末装置によりアクセスされ，該端末装置，該端末装置の鍵交換処理を代行する鍵交換代理装置，または該端末装置と暗号通信を行う通信相手端末からのメッセージを転送するサービス制御装置であって，

前記端末装置，前記鍵交換代理装置，または前記通信相手端末装置からのメッセージを受信するメッセージ受信部と，

前記メッセージ受信部により受信されたメッセージが鍵交換メッセージまたは鍵を含むメッセージかどうかを判断するためのデータを保持し，該データに基づいて前記受信メッセージが前記鍵交換メッセージまたは前記鍵を含むメッセージかどうかを判断し，前記受信メッセージが前記端末装置または通信相手端末装置からの鍵交換メッセージの場合には転送先を前記鍵交換代理装置とし，前記受信メッセージが前記鍵交換代理装置からの鍵交換メッセージの場合には転送先を前記通信相手端末装置とし，前記受信メッセージが前記鍵を含むメッセージの場合には転送先を前記端末装置として決定するプロトコル制御部と，

前記プロトコル制御部により決定された転送先に前記受信メッセージを送信するメッセージ送信部と，

を備えているサービス制御装置。

【０１３２】

（付記８）　付記７において，

前記データは，端末装置ごとに設けられ，アドレスとアプリケーションを指定するポート番号とを含むサービスプロファイルであり，

前記プロトコル制御部は，前記メッセージ受信部により受信されたメッセージの宛先アドレスまたは送信元アドレスと前記サービスプロファイルのアドレス，および，前記受信メッセージに含まれるポート番号と前記サービスプロファイルのポート番号を比較することにより，前記受信メッセージが前記鍵交換メッセージまたは前記鍵を含むメッセージかどうかを判断する，

サービス制御装置。

【０１３３】

（付記９）　通信相手端末装置と暗号通信を行う端末装置に代わって前記通信相手端末との間で鍵交換処理を行う鍵交換代理装置であって，

前記端末装置にアクセスされ，前記端末装置または前記通信相手端末装置からのメッセージを転送するサービス制御装置からのメッセージを受信するメッセージ受信部と，

前記メッセージ受信部により受信されたメッセージが鍵交換メッセージである場合に，前記通信相手端末装置との間で前記鍵交換メッセージを交換して鍵を決定するプロトコル制御部と，

前記プロトコル制御部により決定された前記鍵を，前記鍵を含むメッセージとして前記サービス制御装置宛てに送信するメッセージ送信部と，

を備えている鍵交換代理装置。

【０１３４】

（付記１０）　付記９において，

前記鍵を生成する鍵生成部をさらに備えている鍵交換代理装置。

【０１３５】

（付記１１）　付記９または１０において，

前記プロトコル制御部は，前記端末装置からの鍵交換メッセージの受信を契機として前記通信相手端末装置との間で鍵を決定する，鍵交換代理装置。

【０１３６】

（付記１２）　付記９または１０において，

前記プロトコル制御部は，前記通信相手端末装置からの鍵交換メッセージの受信を契機として前記通信相手端末装置との間で鍵を決定する，鍵交換代理装置。

【０１３７】

（付記１３）　通信ネットワークのサービス制御装置にアクセスして，通信相手端末装置と暗号通信を行う端末装置であって，

暗号化が必要な通信の条件を規定した第１のデータおよび暗号化に使用される鍵を含む第２のデータを保持し，前記第１のデータに基づいて通信相手端末装置との通信に暗号化が必要かどうかを判断し，暗号化に必要な鍵が前記第２のデータに存在するかどうかを判断する暗号処理管理部と，

前記暗号処理管理部により暗号化が必要であると判断され，かつ，暗号化に必要な鍵が存在しないと判断された場合に，鍵交換メッセージを前記サービス制御装置を介して前記通信相手端末宛てに送信するメッセージ送信部と，

前記通信ネットワークの鍵交換代理装置と前記通信相手端末装置との間で決定された鍵を含むメッセージを前記サービス制御装置から受信するメッセージ受信部と，

を備えている端末装置。

【０１３８】

（付記１４）　付記１３において，

前記第１のデータは，暗号化通信が必要な通信相手端末のアドレスと，アプリケーションを指定するポート番号とを含み，

前記暗号処理管理部は，前記通信相手端末装置に送信するメッセージの宛先アドレスと前記第１のデータのアドレス，および，前記送信メッセージに含まれるポート番号と前記第１のデータのポート番号を比較することにより，前記通信相手端末との通信に暗号化が必要かどうかを判断する，

端末装置。

【０１３９】

（付記１５）　付記１３または１４において，

前記第２のデータは，アドレスおよびポート番号，ならびに，暗号化プロトコルおよび暗号化に使用される鍵を含み，

前記暗号処理管理部は，前記第１のデータアドレスと前記第２のデータのアドレス，および，前記第１のデータのポート番号と前記第１のデータのポート番号を比較することにより，暗号化に必要な鍵が前記第２のデータに存在するかどうかを判断する

端末装置。

【０１４０】

（付記１６）　暗号通信を行う第１および第２の端末装置の間で行われる鍵交換処理を前記第１の端末装置に代わって行う鍵交換代理装置および前記第１の端末装置にアクセスされるサービス制御装置を有する鍵交換代理ネットワークシステムで実行される鍵交換代理方法であって，

前記サービス制御装置において，前記第１または第２の端末装置から送信される鍵交換メッセージを前記鍵交換代理装置に転送し，

前記鍵交換代理装置において，前記第１の端末装置と前記第２の端末装置との間で交換される鍵交換メッセージを作成して前記サービス制御装置に送信し，

前記サービス制御装置において，前記鍵交換メッセージを前記第２の端末装置に転送し，

前記鍵交換代理装置において，前記鍵交換メッセージの交換により決定された鍵を含むメッセージを前記サービス制御装置に送信し，

前記サービス制御装置において，前記鍵交換代理装置から送信された前記鍵を含むメッセージを前記第１の端末装置に転送する，

鍵交換代理方法。

【０１４１】

（付記１７）　暗号通信を行う第１および第２の端末装置の間で行われる鍵交換処理を代行する鍵交換代理ネットワークシステムであって，

前記第１の端末装置にアクセスされるサービス制御装置および前記第１の端末装置の鍵交換処理を代行する鍵交換代理装置を備え，

前記サービス制御装置は，受信メッセージの転送先を判断するためのサービス

プロファイルに基づいて，前記第１の端末装置からの鍵交換代理要求メッセージまたは前記第２の端末装置からの鍵交換メッセージを前記鍵交換代理装置に転送し，前記鍵交換代理装置からの鍵交換メッセージを前記第２の端末装置に転送するとともに，前記鍵交換代理装置からの鍵を含むメッセージを前記第１の端末装置に転送し，

前記鍵交換代理装置は，前記鍵交換メッセージを前記第２の端末装置との間で前記サービス制御装置を介して交換して鍵を決定し，決定した鍵を含むメッセージを前記サービス制御装置を介して前記第１の端末装置に送信する，

鍵交換代理ネットワークシステム。

【０１４２】

【発明の効果】

本発明によると，端末装置は，鍵交換および鍵決定に必要な処理を行うことなく，暗号通信に必要な鍵を得ることができ，端末装置の負荷が軽減される。また，端末装置およびその通信相手端末装置のいずから鍵交換処理の要求があっても，ネットワークシステムの鍵交換代理装置（鍵交換代理サーバ）による鍵交換処理の代行が可能である。

【図面の簡単な説明】

【図１】

本発明の実施の形態による鍵交換代理ネットワークシステムの構成を示すブロック図である。

【図２】

サービス制御装置の構成を示すブロック図である。

【図３】

サービスプロファイルの一例を示す。

【図４】

加入者端末の構成を示すブロック図である。

【図５】

（Ａ）は，加入者端末の暗号処理管理部に保持されるＳＰＤを示し，（Ｂ）は加入者端末の暗号処理管理部に保持されるＳＡＤを示している。

【図６】

鍵交換代理サーバの構成を示すブロック図である。

【図７】

加入者端末による鍵交換代理要求メッセージの送信から，加入者端末と通信相手端末との間で暗号化通信が行われるまでの全体のメッセージの流れを示す。

【図８】

加入者端末の詳細な処理の流れを示すシーケンス図である。

【図９】

サービス制御装置に詳細な処理の流れを示すシーケンス図である。

【図１０】

図９のステップＳ１２の詳細な処理の流れを示すフローチャートである。

【図１１】

鍵交換代理サーバの詳細な処理の流れを示すシーケンス図である。

【図１２】

（Ａ）は，加入者端末からサービス制御装置に送信される鍵交換代理要求メッセージの構成を示し，

【図１３】

（Ａ）はサービス制御装置から通信相手端末に送信される鍵交換メッセージを，（Ｂ）は通信相手端末からサービス制御装置に送信される鍵交換メッセージを，（Ｃ）はサービス制御装置から鍵交換代理サーバに送信される鍵交換メッセージを，（Ｄ）は鍵交換代理サーバからサービス制御装置に送信される鍵交換メッセージを，それぞれ示す。

【図１４】

（Ａ）は，鍵交換代理サーバからサービス制御装置に送信される鍵転送メッセージの構成を示し，（Ｂ）は，サービス制御装置から加入者端末に送信される鍵転送メッセージを示す。

【図１５】

鍵が決定された後の加入者端末５のパケットの送受信処理の流れを示すシーケンス図である。

【図１６】

通信相手端末による鍵交換メッセージの送信から，通信相手端末と加入者端末との間で暗号化通信が行われるまでの全体のメッセージの流れを示す。

【符号の説明】

１　サービス制御装置

２　鍵交換代理サーバ

３　認証サーバ

５　加入者端末

６　通信相手端末

７　コアネットワーク

１１，２１，５２　メッセージ送受信部

１２，２２，５４　プロトコル制御部

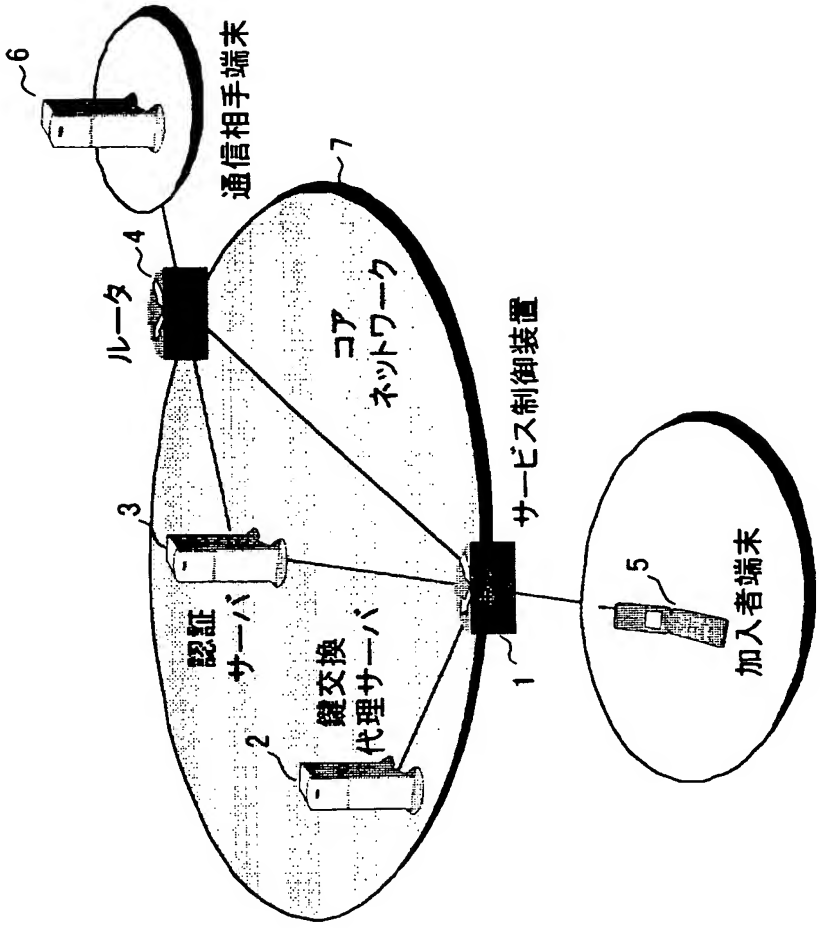
２３　鍵生成部

５３　暗号化／復号化部

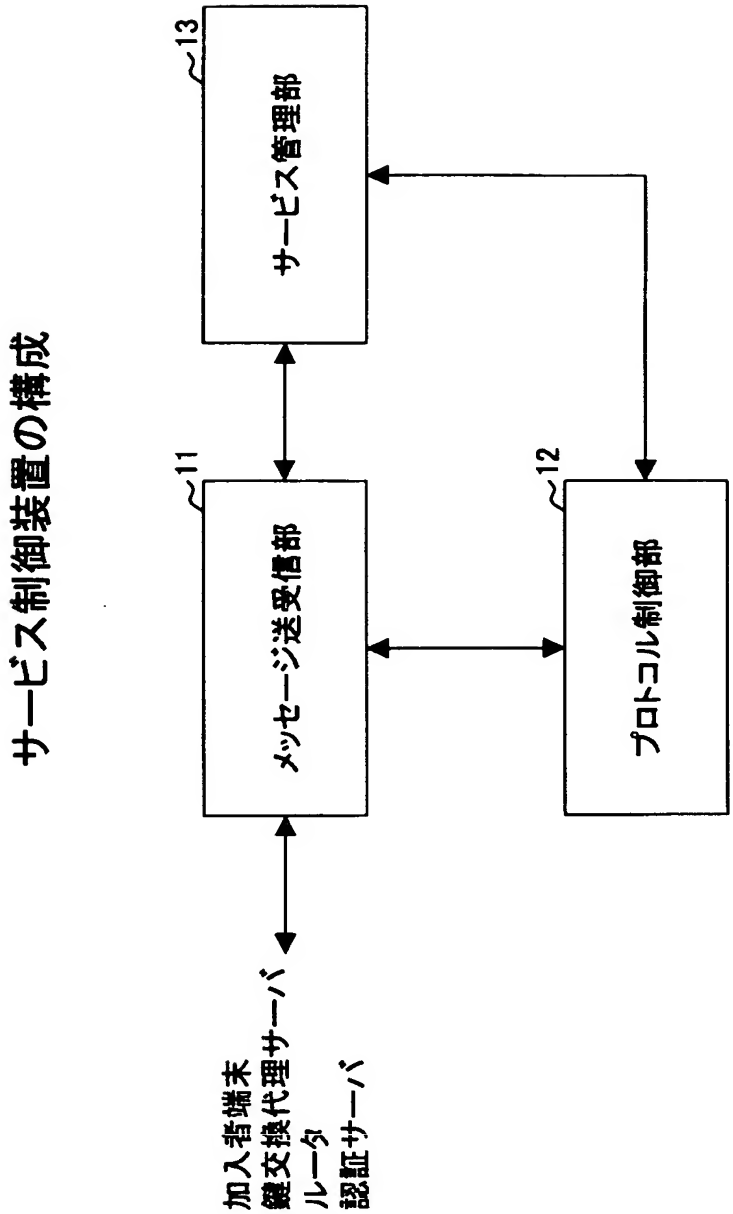
５５　暗号処理管理部

【書類名】　図面

【図１】


6
通信相手端末
7
4
ルータ
コア
ネットワーク
サービス制御装置
3
認証
サーバ
鍵交換
代理サーバ
2
1
5
加入者端末

【図２】

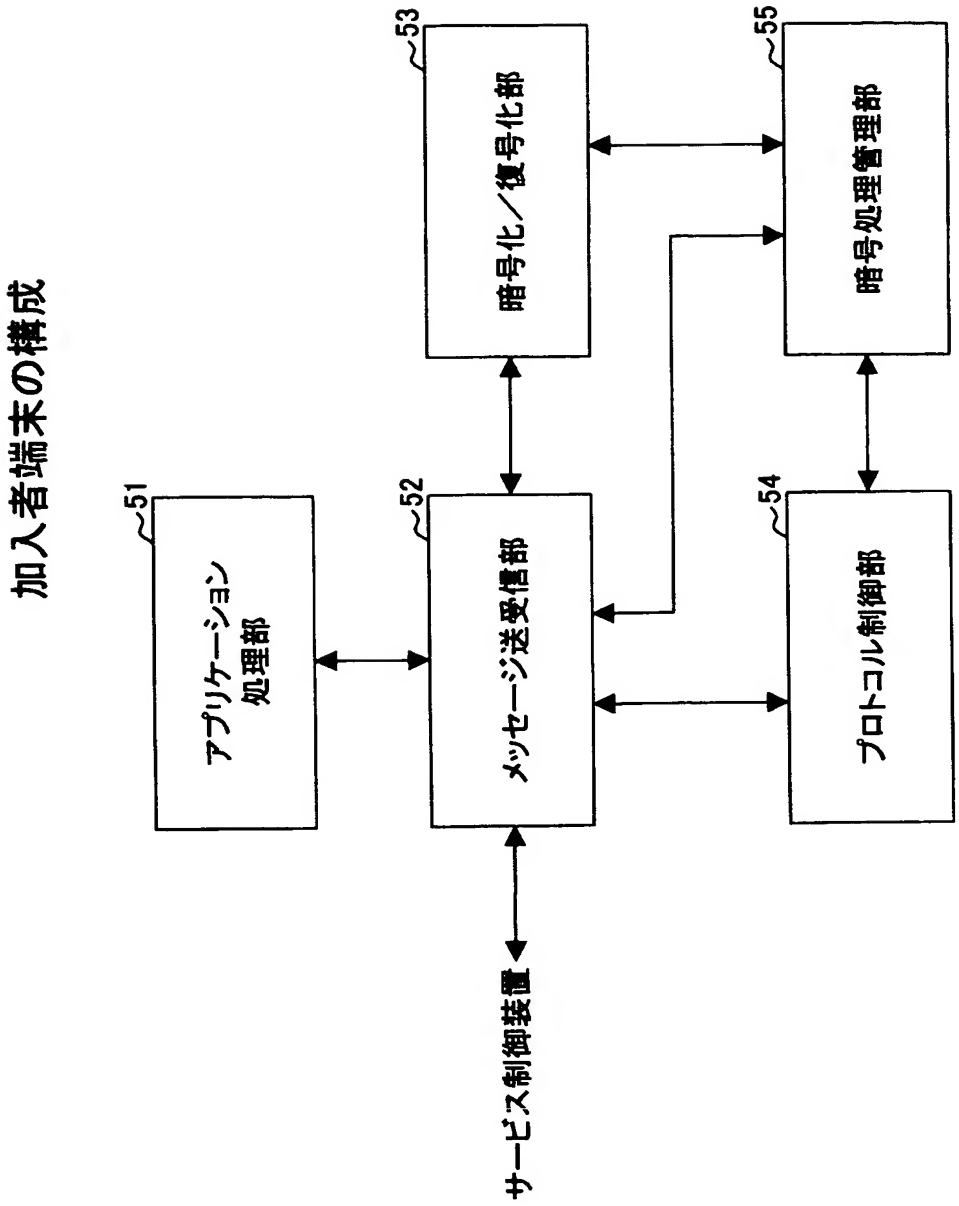

サービス制御装置の構成
13
サービス管理部
11
メッセージ送受信部
12
プロトコル制御部
加入者端末
鍵交換代理サーバ
ルータ
認証サーバ

【図３】

サービスプロファイル

名称	内容
加入者識別情報	電話番号
	NAI
	認証データベースのエントリ番号
	・ ・ ・
IPSec適用条件１	IPアドレス
	ポート番号
IPSec適用条件２	IPアドレス
	ポート番号
・ ・ ・	・ ・ ・

【図４】


加入者端末の構成
53
暗号化／復号化部
55
暗号処理管理部
51
アプリケーション
処理部
52
メッセージ送受信部
54
プロトコル制御部
サービス制御装置

【図５】

加入者端末の保持データ

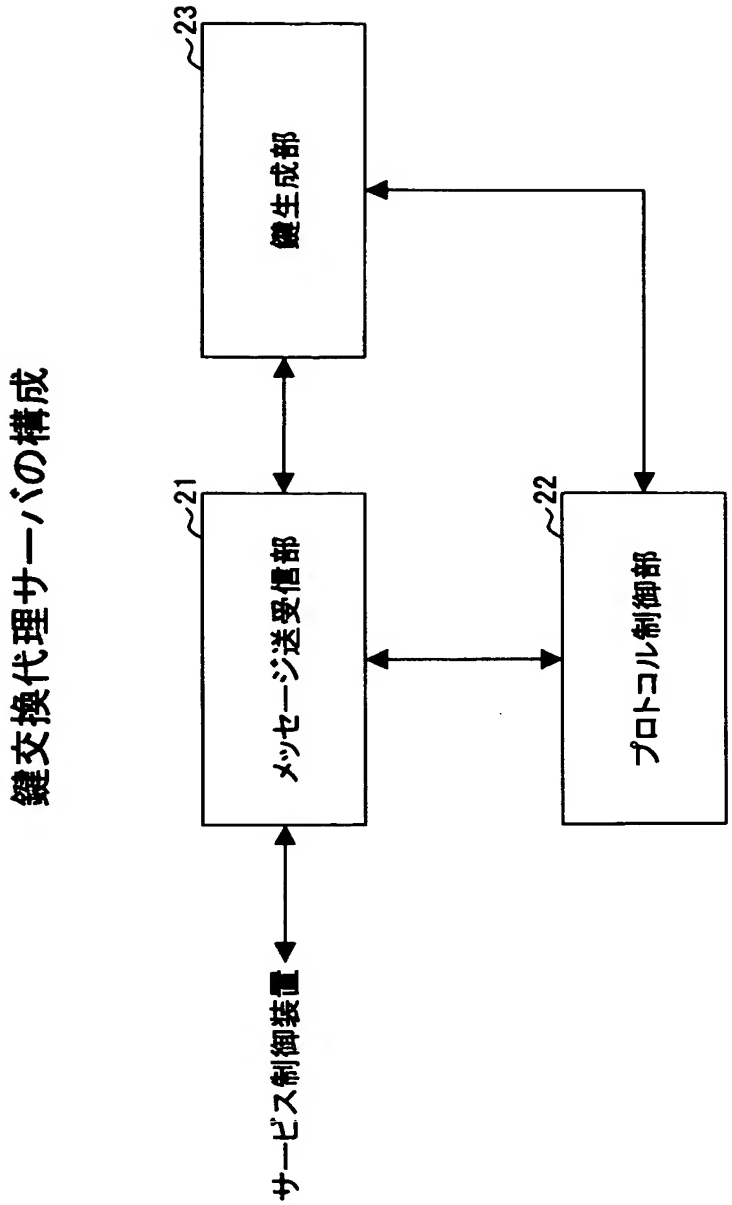
(A)SPD

名称	内容
IPSec適用条件１	IPアドレス
	ポート番号
IPSec適用条件２	IPアドレス
	ポート番号
・ ・ ・	・ ・ ・

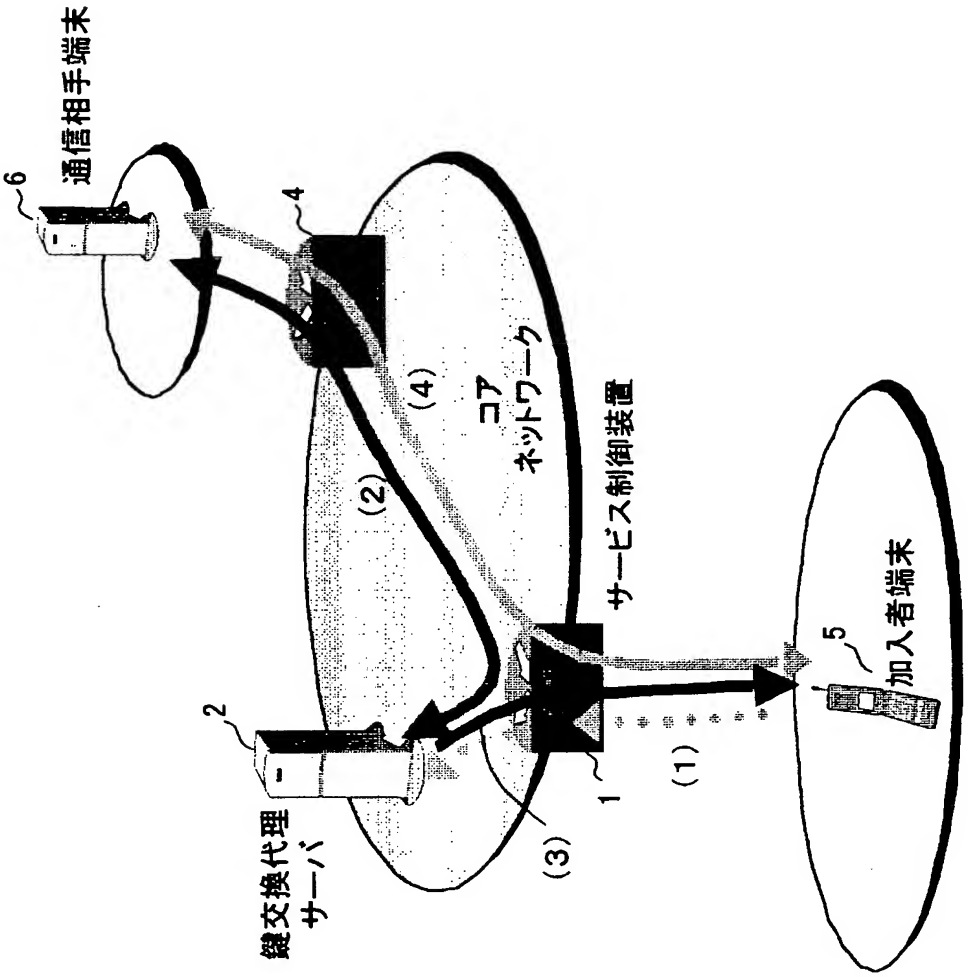
(B)SAD

名称	適用条件	内容
IPSec適用条件１	IPアドレス	暗号化プロトコル
		鍵
	ポート番号	SPI
IPSec適用条件２	IPアドレス	暗号化プロトコル
		鍵
	ポート番号	SPI
・ ・ ・	・ ・ ・	・ ・ ・

【図６】

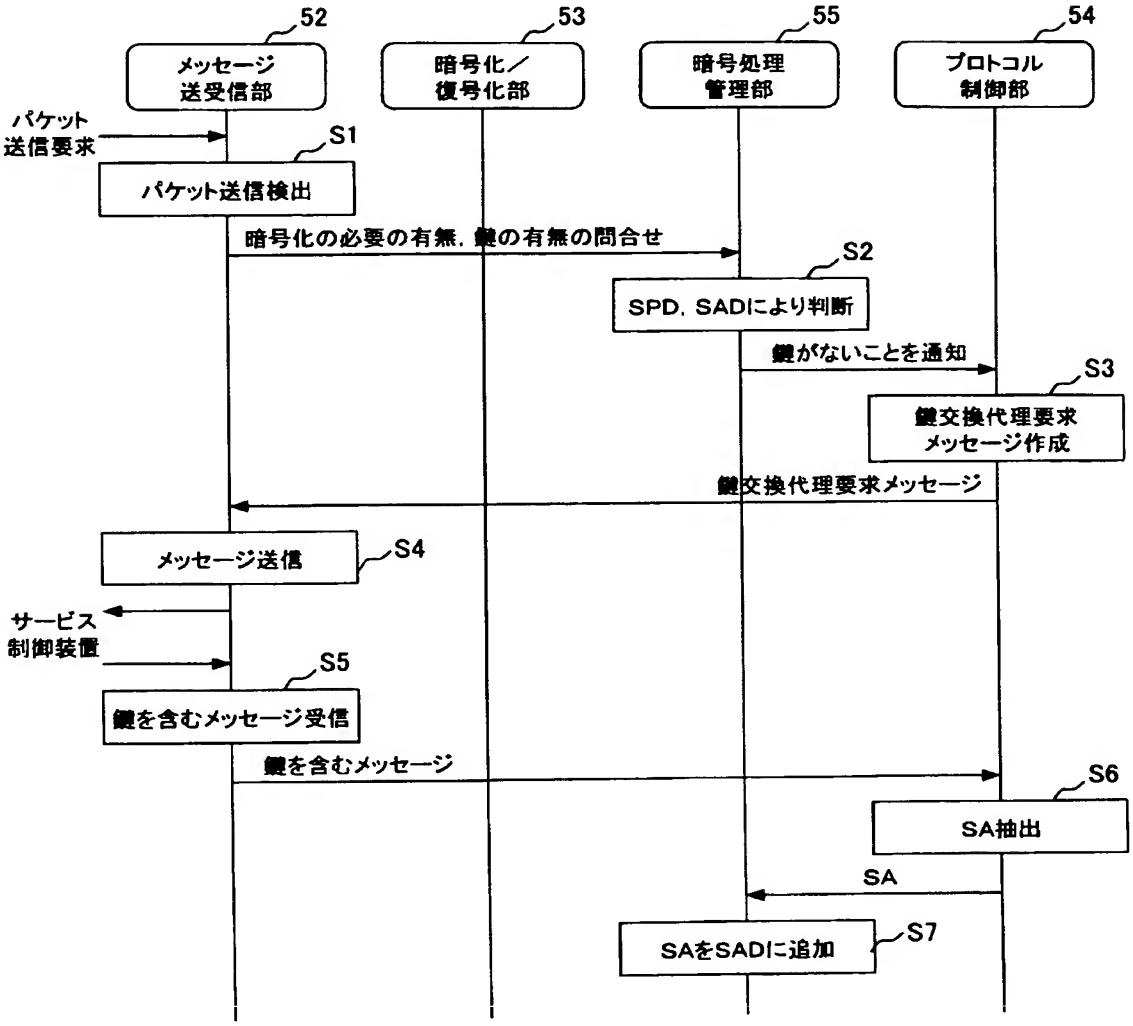


【図７】

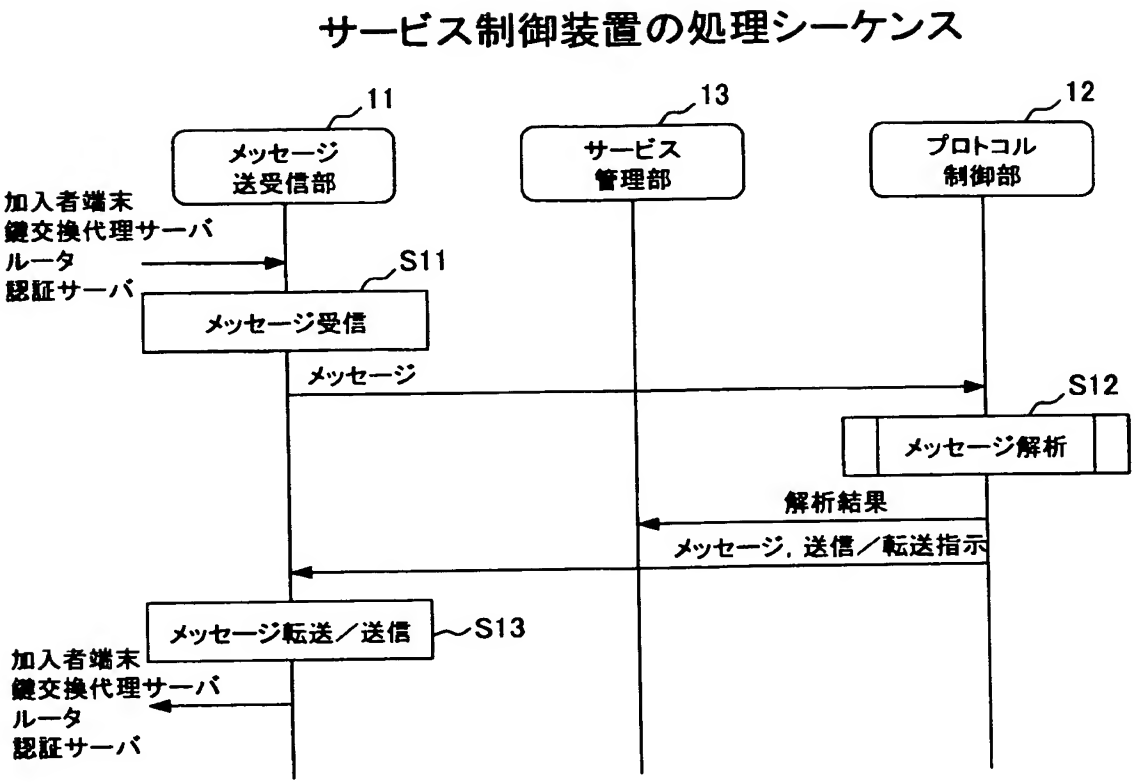


【図８】

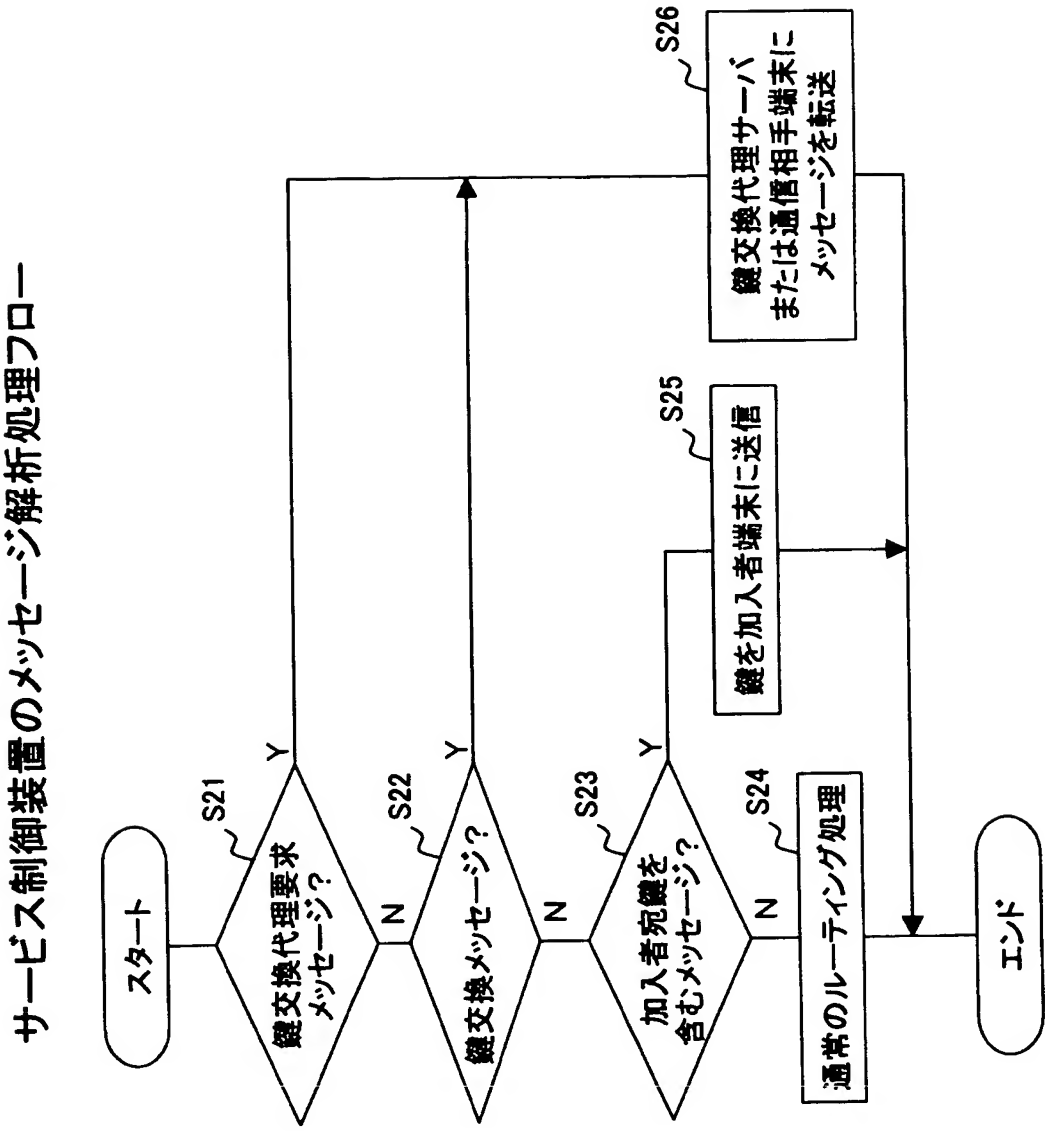
加入者端末の処理シーケンス
（加入者端末からの通信開始時）



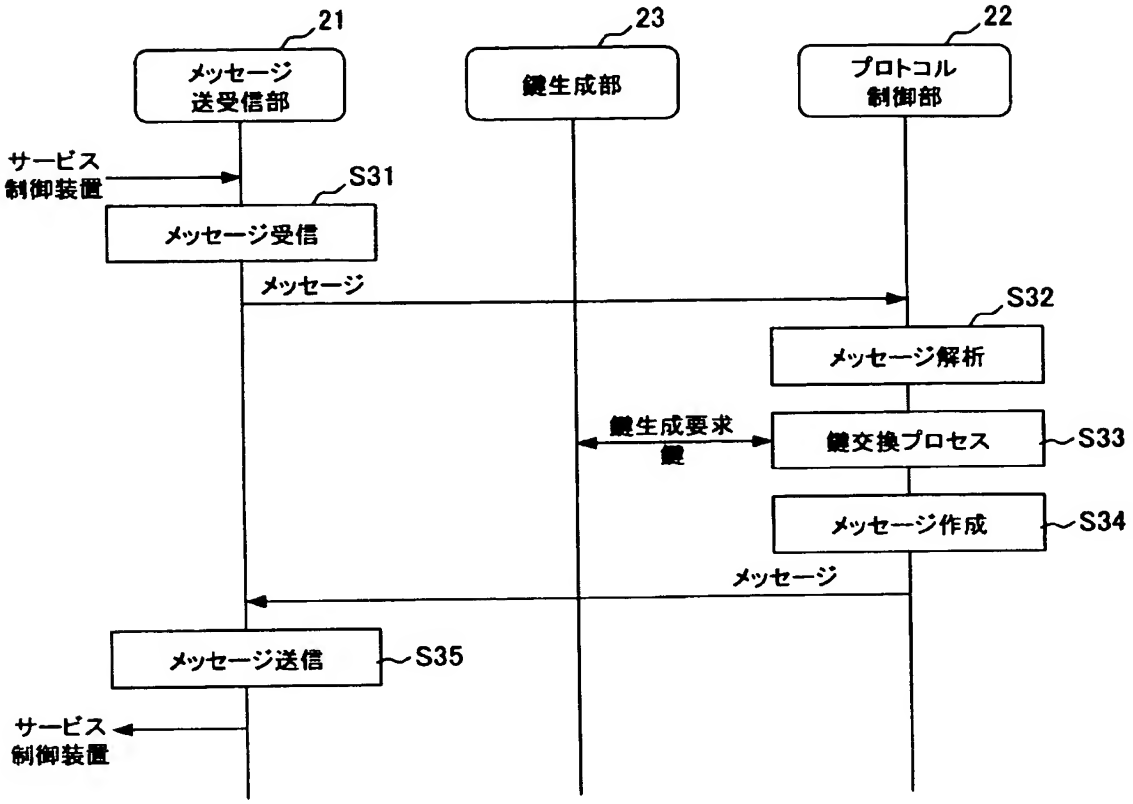
【図９】


サービス制御装置の処理シーケンス
11
メッセージ
送受信部
13
サービス
管理部
12
プロトコル
制御部
加入者端末
鍵交換代理サーバ
ルータ
認証サーバ
S11
メッセージ受信
メッセージ
S12
メッセージ解析
解析結果
メッセージ，送信／転送指示
メッセージ転送／送信
S13
加入者端末
鍵交換代理サーバ
ルータ
認証サーバ

【図１０】


サービス制御装置のメッセージ解析処理フロー
スタート
S21
鍵交換代理要求メッセージ？
Y
N
S22
鍵交換メッセージ？
Y
N
S23
加入者宛鍵を含むメッセージ？
Y
N
S24
通常のルーティング処理
S25
鍵を加入者端末に送信
S26
鍵交換代理サーバまたは通信相手端末にメッセージを転送
エンド

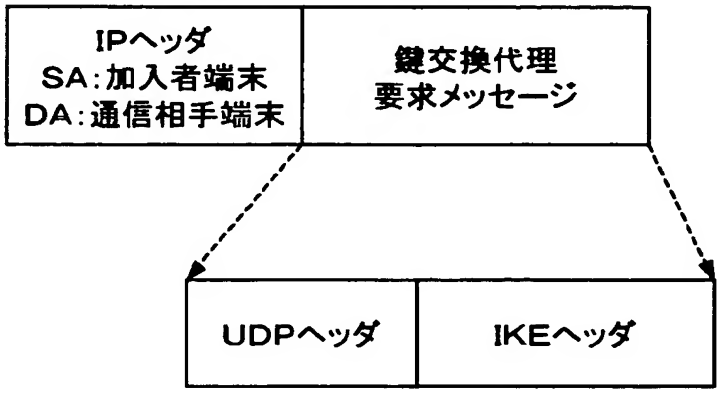
【図１１】


鍵交換代理サーバの処理シーケンス
21
メッセージ
送受信部
23
鍵生成部
22
プロトコル
制御部
サービス
制御装置
S31
メッセージ受信
メッセージ
S32
メッセージ解析
鍵生成要求
鍵
鍵交換プロセス
S33
メッセージ作成
S34
メッセージ
メッセージ送信
S35
サービス
制御装置

【図１２】

（A）鍵交換メッセージ（鍵交換代理要求メッセージ）

（加入者端末→サービス制御装置）



（B）鍵交換メッセージ（鍵交換代理要求メッセージ）

（サービス制御装置→鍵交換代理サーバ）

【図１３】

(A)鍵交換メッセージ

(サービス制御装置→通信相手端末)

IKEメッセージ SA:加入者端末 DA:通信相手端末

(B)鍵交換メッセージ

(通信相手端末→サービス制御装置)

IKEメッセージ SA:通信相手端末 DA:加入者端末

(C)鍵交換メッセージ

(サービス制御装置→鍵交換代理サーバ)

IPヘッダ SA:サービス制御装置 DA:鍵交換代理サーバ	IKEメッセージ SA:通信相手端末 DA:加入者端末

(D)鍵交換メッセージ

(鍵交換代理サーバ→サービス制御装置)

IPヘッダ SA:鍵交換代理サーバ DA:サービス制御装置	IKEメッセージ SA:加入者端末 DA:通信相手端末

【図１４】

（A）鍵転送メッセージ

（鍵交換代理サーバ→サービス制御装置）

IPヘッダ SA:鍵交換代理サーバ DA:サービス制御装置	IPヘッダ SA:通信相手端末 DA:加入者端末	鍵情報(SA)

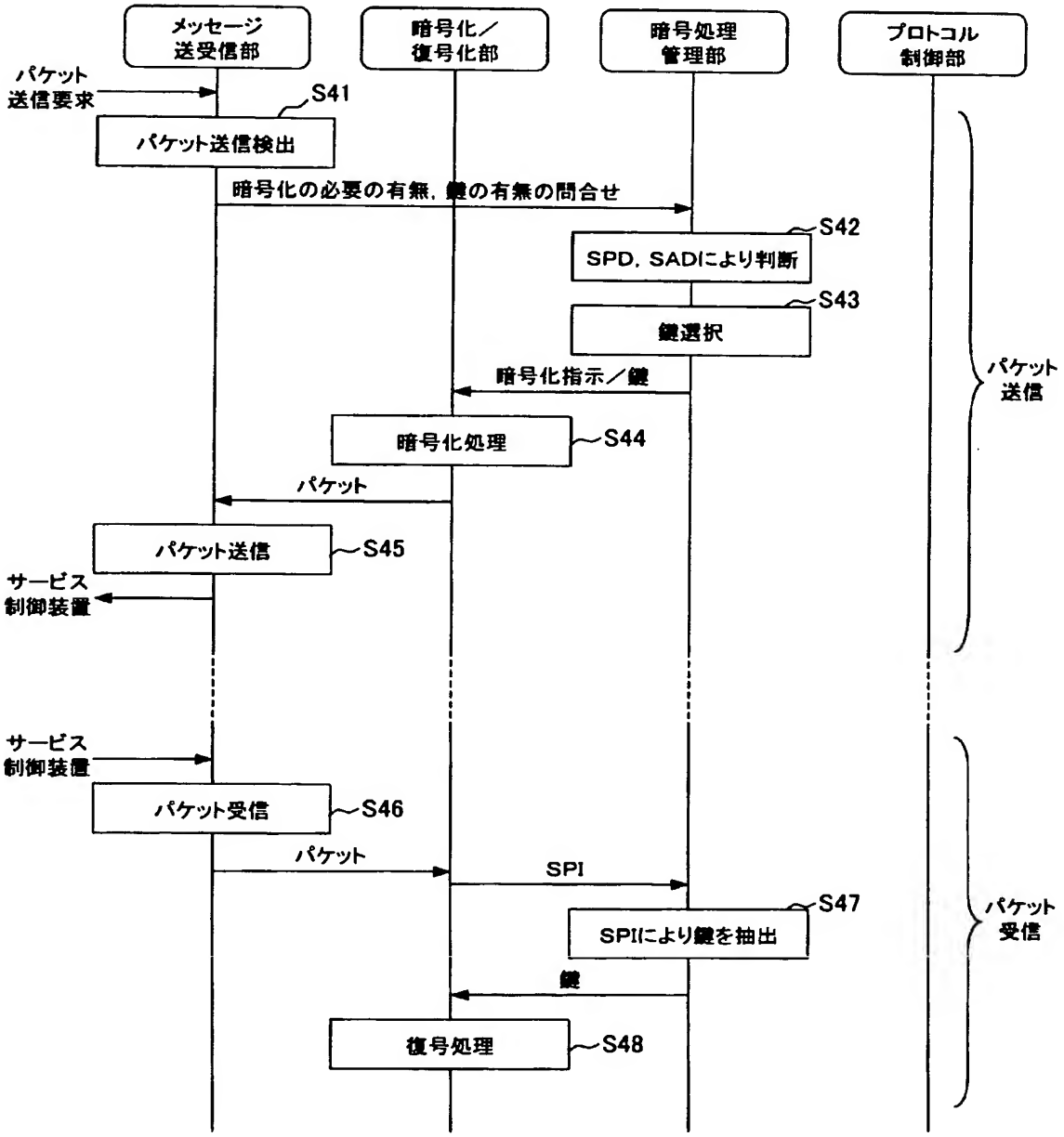
（B）鍵転送メッセージ

（サービス制御装置→加入者端末）

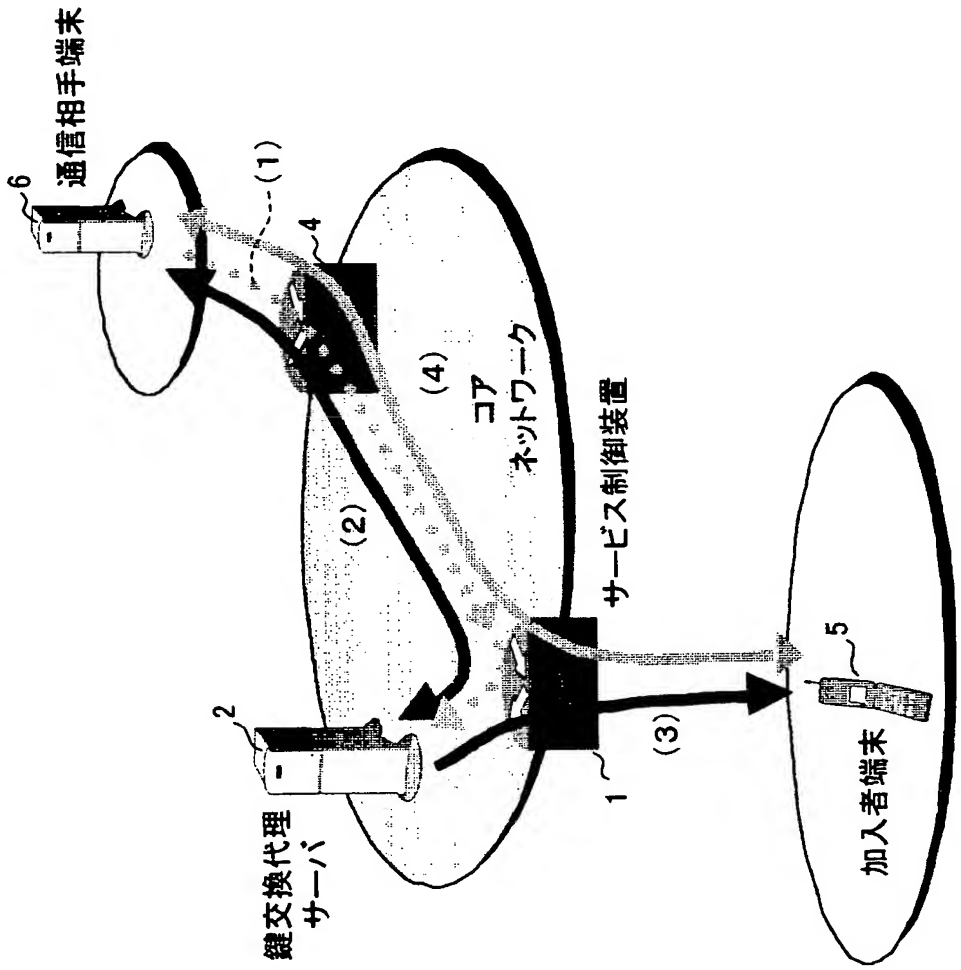
IPヘッダ SA:サービス制御装置 DA:加入者端末	IPヘッダ SA:通信相手端末 DA:加入者端末	鍵情報(SA)

【図１５】

加入者端末の処理シーケンス
（パケット送受信）



【図１６】



【書類名】　要約書

【要約】

【課題】　鍵交換に伴う処理をネットワーク側の装置に代行させて，端末の負荷を軽減する。

【解決手段】　加入者端末５は，通信相手端末６との間で行う通信の暗号化に必要な暗号鍵を保持しない場合に，鍵交換代理要求メッセージをサービス制御装置１に送信する。サービス制御装置１は，認証サーバ３から与えられたサービスプロファイルに基づいて，鍵交換代理要求メッセージを鍵交換代理サーバ２に転送する。鍵交換代理サーバ２は，鍵交換メッセージを通信相手端末６との間で送受信して鍵を決定し，決定した鍵を含むメッセージをサービス制御装置１に送信する。サービス制御装置１は，鍵交換代理サーバ２からの鍵を含むメッセージをサービスプロファイルに基づいて加入者端末５に転送する。その後，加入者端末５と通信相手端末６との間で，暗号化通信が行われる。

【選択図】　図１

特願２００２－２８８４７６

出　願　人　履　歴　情　報

識別番号　　［０００００５２２３］

１．変更年月日　　１９９０年　８月２４日
［変更理由］　新規登録
住　所　神奈川県川崎市中原区上小田中１０１５番地
氏　名　富士通株式会社

２．変更年月日　　１９９６年　３月２６日
［変更理由］　住所変更
住　所　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　富士通株式会社